



Política de Gestión Integral de Riesgos Institucionales Versión 3

Justicia Penal Militar y Policial

2026



	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 2 de 64
---	---	---

Contenido

Introducción	4
1. Declaración de Política	5
2. Objetivo	6
3. Alcance.....	6
4. Definiciones	7
5. Marco normativo	13
6. Roles y responsabilidades.....	15
6.1 Gobierno del Riesgo	15
6.2 Roles y responsabilidades	17
7. Análisis de contexto (interno y externo).....	18
8. Política de gestión integral del riesgo.	29
9. Apetito, tolerancia y capacidad de riesgo.....	31
9.1 Criterios institucionales de aceptación del riesgo.....	32
9.2 Niveles de aceptación del riesgo	32
9.2.1 Estrategia para combatir el riesgo	34
9.3 Umbral del riesgo	34
9.4 Indicadores Clave de Proceso (KPI) e Indicadores Clave de Riesgo (KRI) 35	
9.4.1 Alcance Indicadores KPI e KRI	36
9.4.2 Criterios para la formulación, seguimiento y monitoreo de los KRI. 36	
9.5 Revisión y actualización.....	40
10. Metodología para la gestión integral del riesgo.	40
10.1 Identificación y descripción del riesgo	42
10.1.1 Descripción del riesgo	43
10.2 Análisis de riesgo inherente.....	45
10.2.1 Probabilidad	46

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 3 de 64
---	---	---

10.2.2	Impacto	46
	Análisis de severidad	47
10.3	Diseño y análisis de controles	48
10.3.1	Estructura para la Descripción del Control.....	49
10.3.2	Tipos de control:	50
10.3.3	Criterios de valoración de controles	51
10.4	Valoración de Riesgo Residual	51
10.4.1	Consolidación Mapa de Riesgos Institucional:	52
11.	Gestión preventiva de riesgos fiscales.....	52
12.	Riesgos de Seguridad de la Información	53
13.	Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP	54
13.1	Riesgos para la Integridad Pública	55
14.	Tratamiento y control de los riesgos fiscales, de seguridad de la información y de integridad pública.	56
15.	Opciones de Manejo del Riesgo	57
16.	Acciones ante los riesgos materializados	60
17.	Monitoreo, seguimiento auditoría y supervisión al mapa de riesgos institucional y controles.	61
17.1	Mejora continua	62
18.	Anexos.	63

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 4 de 64
---	---	---------------------------

Introducción

La Política para la Gestión Integral de Riesgos Institucionales de la Justicia Penal Militar y Policial tiene como propósito fortalecer la identificación, análisis, evaluación, tratamiento, monitoreo y seguimiento de los riesgos que puedan afectar el cumplimiento de los objetivos estratégicos, la prestación de los servicios y la generación de valor público, promoviendo una cultura de prevención, transparencia, integridad y mejora continua en el marco de sus competencias constitucionales y legales. Esta política se fundamenta en lo dispuesto por la Constitución Política de Colombia, la Ley 87 de 1993¹, la Ley 489 de 1998², la Ley 1474 de 2011³, la Ley 1712 de 2014⁴, la Ley 2195 de 2022⁵, el Decreto 1499 de 2017⁶ y el Decreto 1122 de 2024⁷, así como en los lineamientos emitidos por el Departamento Administrativo de la Función Pública para la implementación del Modelo Integrado de Planeación y Gestión – MIPG y el Sistema de Control Interno.

En desarrollo de estas disposiciones y como parte de la implementación del MIPG, la Entidad cuenta con el Comité Institucional de Gestión y Desempeño, adoptado mediante la Resolución 000023 de 2024⁸, el cual, en articulación con el Comité Institucional de Coordinación de Control Interno, reglamentado por el artículo 13 de la Ley 87 de 1993 y adoptado mediante las Resoluciones 000282⁹ y 000990 de 2024¹⁰, se constituye en una instancia fundamental para la orientación, análisis y toma de decisiones asociadas a la gestión integral de riesgos, el fortalecimiento institucional y la mejora continua de la gestión pública.

La presente política se desarrolla conforme a los lineamientos establecidos en la **Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7-2025 (Guía-GIR V7)**¹¹, expedida por el Departamento Administrativo de la Función Pública, la cual incorpora un enfoque integral para la gestión de riesgos

¹ Congreso de la República de Colombia. (1993). 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. Diario Oficial No. 41.120.

² Congreso de la República de Colombia. (1998). Ley 489 de 1998. Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional. Diario Oficial No. 43.464.

³ Congreso de la República de Colombia. (2011). 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. Diario Oficial No. 48.128.

⁴ Congreso de la República de Colombia. (2014). 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. Diario Oficial No. 49.084.

⁵ Congreso de la República de Colombia. (2022). 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. Diario Oficial No. 51.921.

⁶ Presidencia de la República de Colombia. (2017). Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015 en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015. Bogotá D.C., Colombia.

⁷ Presidencia de la República de Colombia. (2024). 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. Bogotá D.C., Colombia.

⁸ Unidad Administrativa Especial de la Justicia Penal Militar y Policial. (2024). Resolución 000023 de 2024. Por la cual se adopta el Comité Institucional de Gestión y Desempeño.

⁹ Unidad Administrativa Especial de la Justicia Penal Militar y Policial. (2024). Resolución 000282 de 2024. Por la cual se adopta el Comité Institucional de Coordinación de Control Interno.

¹⁰ Unidad Administrativa Especial de la Justicia Penal Militar y Policial. (2024). Resolución 000990 de 2024. Por la cual se actualizan disposiciones relacionadas con el Comité Institucional de Coordinación de Control Interno.

¹¹ Departamento Administrativo de la Función Pública. (2025). Guía para la Gestión Integral del Riesgo en Entidades Públicas. Versión 7. Bogotá D.C., Colombia.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 5 de 64
---	---	---

institucionales, fiscales, de integridad pública, de corrupción, de seguridad de la información y de ciberseguridad, en concordancia con las disposiciones del Programa de Transparencia y Ética Pública (PTEP), el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) y las mejores prácticas internacionales en materia de gestión del riesgo basadas en el enfoque COSO ERM¹².

Asimismo, esta política reconoce la gestión del riesgo como un componente estratégico de la gobernanza institucional, orientado a fortalecer la capacidad de la Entidad para anticipar, prevenir, detectar y responder oportunamente a situaciones que puedan afectar el cumplimiento de los objetivos institucionales, la adecuada gestión de los recursos públicos, la prestación de los servicios, la seguridad de la información, la continuidad de la operación y la confianza de los grupos de valor. Para ello, se articula con el esquema de líneas de defensa, promoviendo la responsabilidad compartida de los servidores públicos y contratistas en la identificación y gestión de los riesgos asociados a los procesos institucionales.

En consecuencia, la Política de Gestión Integral de Riesgos Institucional establece el marco general para la adopción de controles, la implementación de acciones de tratamiento y el fortalecimiento de mecanismos de seguimiento y evaluación que contribuyan a reducir la exposición a riesgos, incrementar la resiliencia organizacional y garantizar el cumplimiento efectivo de la misión institucional, en observancia de los principios de legalidad, eficiencia, transparencia, responsabilidad y protección del patrimonio público.

1. Declaración de Política

La Justicia Penal Militar y Policial se compromete a integrar la Gestión Integral del Riesgo en todos los niveles de la gestión institucional como un elemento estratégico para la toma de decisiones, el fortalecimiento del Sistema de Control Interno, la protección de los recursos públicos, la generación de valor público y el cumplimiento de sus objetivos institucionales.

Para ello, promoverá una cultura organizacional basada en la prevención, la transparencia, la integridad, la responsabilidad, el autocontrol y la mejora continua, asegurando la gestión oportuna y efectiva de los riesgos institucionales, de corrupción, integridad pública, fiscales, seguridad de la información, seguridad digital y demás riesgos que puedan afectar el logro de la misión institucional.

¹² La presente Política de Administración de Riesgos Institucional adopta los principios del marco COSO ERM (Enterprise Risk Management) como referente internacional para la gestión integral del riesgo, promoviendo su integración con la estrategia, la gobernanza, el desempeño institucional y la toma de decisiones, en concordancia con los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 expedida por el Departamento Administrativo de la Función Pública.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 6 de 64
---	---	---

Asimismo, garantizará la aplicación del esquema de Línea Estratégica y Líneas de Defensa, la articulación con el Programa de Transparencia y Ética Pública (PTEP), el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), el Modelo Integrado de Planeación y Gestión (MIPG) y los demás instrumentos institucionales aplicables, con el propósito de fortalecer la capacidad institucional para anticipar, gestionar y responder de manera oportuna a los riesgos derivados de la incertidumbre.

De igual forma, la entidad promoverá la identificación y aprovechamiento de oportunidades que contribuyan al fortalecimiento institucional, la innovación, la transformación digital, la mejora de los procesos, la optimización de los recursos y la generación de valor público, como resultado del análisis permanente del contexto y de la gestión integral del riesgo.

2. Objetivo

Establecer el marco institucional para la Gestión Integral del Riesgo en la Justicia Penal Militar y Policial (JPMP), definiendo los lineamientos, responsabilidades y mecanismos necesarios para identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos de gestión, corrupción, fiscales, seguridad de la información, seguridad digital, continuidad del negocio y demás riesgos aplicables, con el fin de disminuir la vulnerabilidad institucional, el logro de los objetivos estratégicos, fortalecer la capacidad institucional para anticipar y gestionar eventos de incertidumbre, proteger los recursos públicos, mejorar el desempeño institucional y asegurar la generación de valor público en cumplimiento de la misión de la Entidad.

3. Alcance

La presente Política de Gestión Integral del Riesgo aplica a todos los procesos, dependencias, servidores públicos, contratistas, proyectos, programas, terceros, convenios y particulares que puedan generar riesgos en las actividades desarrolladas para la Justicia Penal Militar y Policial (JPMP), constituyéndose en el marco institucional para la gestión de los riesgos que puedan afectar el cumplimiento de los objetivos estratégicos, misionales, operativos y de apoyo, la prestación del servicio, la protección de los recursos públicos y la generación de valor público.

Su aplicación comprende la gestión de los riesgos institucionales, de corrupción, integridad pública, fiscales, seguridad de la información, seguridad digital y demás riesgos asociados al desarrollo de los procesos institucionales, de

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 7 de 64
---	---	---------------------------

conformidad con la normatividad vigente y los lineamientos definidos por la Entidad.

Los lineamientos establecidos en esta política deberán ser observados por la Línea Estratégica y las Líneas de Defensa, en el marco de las responsabilidades definidas para cada una de ellas, promoviendo una cultura institucional basada en la prevención, el autocontrol, la transparencia y la mejora continua.

La Gestión Integral del Riesgo se desarrollará de manera articulada con el Modelo Integrado de Planeación y Gestión (MIPG), el Sistema de Control Interno, el Programa de Transparencia y Ética Pública (PTEP), el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), la Política de Seguridad Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los demás instrumentos institucionales que contribuyan al fortalecimiento de la gestión y al cumplimiento de los objetivos de la Entidad.

4. Definiciones¹³

Para efectos de la presente Política de Gestión Integral de Riesgos Institucionales, se adoptan las siguientes definiciones, alineadas con la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025), el marco COSO ERM 2017, el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo de Seguridad y Privacidad de la Información (MSPI), la Ley 2195 de 2022 y el Decreto 1122 de 2024.

Activo: Elemento que posee valor para la entidad y requiere protección, incluyendo información, software, hardware, servicios, personas, procesos e infraestructura tecnológica¹⁴.

Administración del Riesgo: Proceso sistemático para identificar, analizar, evaluar, tratar, monitorear y comunicar riesgos que puedan afectar el logro de los objetivos institucionales¹⁵.

Alta Dirección: Instancia responsable de orientar, aprobar y supervisar la Gestión Integral del Riesgo, asegurando su alineación con la estrategia institucional y el Sistema de Control Interno¹⁶.

¹³ Las definiciones contenidas en la presente Política de Gestión Integral del Riesgo fueron adoptadas y adaptadas de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025), el Modelo Integrado de Planeación y Gestión (MIPG), el marco COSO ERM 2017, la Ley 2195 de 2022, el Decreto 1122 de 2024, la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI), la Norma ISO 31000:2018 y la Norma ISO 37001.

¹⁴ Guía GIR V7.

¹⁵ Guía GIR V7.

¹⁶ MIPG; COSO ERM 2017.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 8 de 64
---	---	--

Alerta Temprana: Señal o indicador que permite advertir oportunamente cambios en la exposición al riesgo o la posible ocurrencia de eventos que puedan afectar el cumplimiento de los objetivos institucionales¹⁷.

Apetito del Riesgo: Nivel de riesgo que la entidad está dispuesta a asumir para alcanzar sus objetivos institucionales¹⁸.

Bien Público: Bienes muebles e inmuebles de propiedad pública y productos derivados del ejercicio de una función pública¹⁹.

Capacidad de Riesgo: Nivel máximo de riesgo que una entidad puede soportar considerando sus recursos, capacidades y obligaciones legales²⁰.

Causa: Factores internos o externos que pueden generar o propiciar la materialización de un riesgo²¹.

Causa Inmediata: Circunstancia que favorece la ocurrencia del riesgo sin constituir su origen principal²².

Causa Raíz: Razón fundamental u origen principal que da lugar a la ocurrencia del riesgo²³.

Ciberseguridad: Conjunto de prácticas, controles y capacidades encaminadas a proteger activos, sistemas y servicios digitales frente a amenazas del ciberespacio²⁴.

Conflicto de Interés: Situación en la cual un interés particular, directo o indirecto, puede influir o parecer influir en el ejercicio imparcial y objetivo de una función pública²⁵.

Consecuencia: Efecto o resultado que se produce cuando un riesgo se materializa²⁶.

Contexto del Riesgo: Condiciones internas y externas que influyen en el logro de los objetivos y en la gestión de los riesgos²⁷.

¹⁷Guía GIR V7.

¹⁸ Guía GIR V7 – COSO ERM.

¹⁹ Ley 610 de 2000.

²⁰ COSO ERM 2017; Guía DAFP V7.

²¹ Guía GIR V7.

²² Guía GIR V7.

²³ Guía GIR V7.

²⁴ Política de Gobierno Digital.

²⁵ Ley 2195 de 2022; Decreto 1122 de 2024.

²⁶ Guía GIR V7.

²⁷ ISO 31000:2018; Guía DAFP V7.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 9 de 64
---	---	---

Continuidad del Negocio: Capacidad de la Entidad para mantener o restablecer la prestación de sus funciones y servicios esenciales dentro de niveles aceptables previamente definidos frente a eventos disruptivos²⁸.

Control: Medida, acción o mecanismo diseñado para prevenir, detectar o mitigar la probabilidad o impacto de un riesgo²⁹.

Cultura del Riesgo: Conjunto de valores, comportamientos y actitudes que influyen en la forma como la entidad comprende y gestiona los riesgos³⁰.

Debida Diligencia: Proceso mediante el cual se identifican, evalúan y gestionan riesgos asociados a corrupción, soborno, fraude, conflictos de interés, terceros y otras situaciones que puedan afectar la integridad institucional³¹.

Efecto: Daño potencial que se genera sobre los recursos públicos, bienes o intereses patrimoniales del Estado³².

Evento Potencial: Hecho incierto que puede ocurrir y afectar el cumplimiento de los objetivos institucionales o los recursos públicos³³.

Factores de Riesgo: Fuentes, circunstancias o situaciones que generan exposición al riesgo³⁴.

Fraude: Acto intencional realizado para obtener un beneficio indebido mediante engaño, abuso de confianza, ocultamiento u otra conducta irregular³⁵.

Gestión de Riesgos Emergentes: Proceso orientado a identificar, analizar y monitorear riesgos derivados de cambios en el contexto interno o externo de la Entidad³⁶.

Gestión Integral del Riesgo: Conjunto de políticas, metodologías, herramientas y actividades orientadas a gestionar integralmente los riesgos institucionales³⁷.

Gobierno del Riesgo: Estructuras, responsabilidades y mecanismos mediante los cuales la alta dirección orienta y supervisa la gestión de riesgos³⁸.

²⁸ ISO 22301; Guía DAFP V7.

²⁹ Guía GIR V7.

³⁰ COSO ERM 2017

³¹ Ley 2195 de 2022; Decreto 1122 de 2024; ISO 37001.

³² Guía GIR V7 – Riesgo Fiscal.

³³ Guía GIR V7 – Riesgo Fiscal.

³⁴ Guía GIR V7.

³⁵ COSO ERM 2017; Ley 2195 de 2022.

³⁶ Guía DAFP V7.

³⁷ Guía GIR V7.

³⁸ COSO ERM 2017; Guía DAFP V7.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 10 de 64
---	---	----------------------------

Identificación del Riesgo: Actividad mediante la cual se reconocen y describen los eventos que pueden afectar los objetivos institucionales³⁹.

Indicador Clave de Riesgo (KRI): Métrica utilizada para generar alertas tempranas sobre cambios en la exposición al riesgo⁴⁰.

Integridad Pública: Adhesión y coherencia entre principios, valores y comportamientos esperados en el ejercicio de la función pública⁴¹.

Líneas de Defensa: Modelo de responsabilidades para gestionar, monitorear y evaluar riesgos mediante la actuación coordinada de la línea estratégica, primera, segunda y tercera línea de defensa⁴².

Mapa de Riesgos: Herramienta que consolida la identificación, análisis, evaluación, valoración y tratamiento de los riesgos institucionales⁴³.

Materialización del Riesgo: Ocurrencia real de un evento de riesgo que genera consecuencias sobre los objetivos institucionales⁴⁴.

MIPG: Modelo Integrado de Planeación y Gestión que articula la gestión institucional orientada a resultados y generación de valor público⁴⁵.

Monitoreo del Riesgo: Seguimiento periódico a los riesgos, controles y acciones de tratamiento para verificar su efectividad⁴⁶.

Nivel de Madurez de la Gestión del Riesgo: Grado de desarrollo e implementación de la gestión integral del riesgo en una organización⁴⁷.

Nivel de Riesgo: Resultado de combinar la probabilidad de ocurrencia y el impacto del riesgo⁴⁸.

Oportunidad: Circunstancia o conjunto de circunstancias derivadas de la incertidumbre, del análisis del contexto o de la gestión integral del riesgo, que pueden generar efectos favorables para el cumplimiento de los objetivos institucionales, la mejora del desempeño, la innovación, la optimización de los recursos o la generación de valor público⁴⁹.

³⁹ Guía GIR V7.

⁴⁰ COSO ERM 2017.

⁴¹ Decreto 1122 de 2024 – SIGRIP; Ley 2195 de 2022.

⁴² MIPG – Guía GIR V7.

⁴³ Guía GIR V7.

⁴⁴ Guía GIR V7.

⁴⁵ Decreto 1499 de 2017.

⁴⁶ Guía GIR V7.

⁴⁷ COSO ERM – Herramienta de Madurez DAFP.

⁴⁸ Guía GIR V7.

⁴⁹ Guía GIR V7; COSO ERM 2017 y la ISO 31000:2018.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 11 de 64
---	---	---

Probabilidad: Posibilidad de ocurrencia de un evento de riesgo⁵⁰.

Programa de Transparencia y Ética Pública (PTEP): Instrumento de planeación que integra acciones para fortalecer la transparencia, la integridad y la lucha contra la corrupción⁵¹.

Recurso Público: Recursos financieros, físicos, tecnológicos y patrimoniales administrados por las entidades públicas⁵².

Riesgo: Efecto de la incertidumbre sobre el logro de los objetivos institucionales⁵³.

Riesgo de Ciberseguridad: Posibilidad de afectación de activos digitales, sistemas o servicios derivada de amenazas del ciberespacio⁵⁴.

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se utilice el poder para desviar la gestión de lo público hacia un beneficio privado o indebido⁵⁵.

Riesgo de Integridad Pública: Posibilidad de ocurrencia de eventos que afecten los principios y valores que orientan el ejercicio de la función pública⁵⁶.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza explote una vulnerabilidad afectando la confidencialidad, integridad o disponibilidad de la información⁵⁷.

Riesgo Estratégico: Posibilidad de ocurrencia de eventos que afecten el direccionamiento estratégico, la generación de valor público o el cumplimiento de los objetivos institucionales⁵⁸.

Riesgo Fiscal: Efecto dañoso potencial sobre recursos públicos, bienes o intereses patrimoniales de naturaleza pública⁵⁹.

Riesgo Inherente: Nivel de riesgo existente antes de aplicar controles⁶⁰.

⁵⁰ Guía GIR V7.

⁵¹ Decreto 1122 de 2024.

⁵² Guía GIR V7 – Riesgo Fiscal; Ley 610 de 2000.

⁵³ Guía GIR V7 – COSO ERM; ISO 31000:2018.

⁵⁴ Política de Gobierno Digital.

⁵⁵ Ley 1474 de 2011, Ley 2195 de 2022 y Guía GIR V7.

⁵⁶ Decreto 1122 de 2024 – SIGRIP.

⁵⁷ MSPI; ISO 27001:2022.

⁵⁸ COSO ERM 2017.

⁵⁹ Ley 610 de 2000; Decreto Ley 403 de 2020.

⁶⁰ Guía GIR V7.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 12 de 64
---	---	----------------------------

Riesgo Operacional: Posibilidad de afectaciones derivadas de fallas en procesos, personas, tecnología, infraestructura o acontecimientos externos⁶¹.

Riesgo Residual: Nivel de riesgo que permanece después de aplicar controles y evaluar su efectividad⁶².

Riesgos Emergentes: Riesgos nuevos o en evolución cuya probabilidad o impacto puede incrementarse debido a cambios en el contexto interno o externo⁶³.

Seguridad Digital: Preservación de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y los servicios digitales mediante la gestión de riesgos y controles de seguridad⁶⁴.

SIGRIP: Sistema de Gestión de Riesgos para la Integridad Pública orientado a identificar, analizar, tratar y monitorear riesgos asociados a la integridad pública⁶⁵.

Soborno: Oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida para influir en una decisión o actuación relacionada con el ejercicio de funciones o actividades institucionales⁶⁶.

Terceros: Personas naturales o jurídicas externas a la Entidad que interactúan con esta mediante contratos, convenios, alianzas u otras relaciones institucionales⁶⁷.

Tolerancia al Riesgo: Variación aceptable respecto del logro de los objetivos institucionales frente a la exposición al riesgo⁶⁸.

Tratamiento del Riesgo: Acciones implementadas para evitar, reducir, compartir, transferir o aceptar riesgos⁶⁹.

Valoración del Riesgo: Resultado del análisis y evaluación de la probabilidad y el impacto del riesgo⁷⁰.

⁶¹ ISO 31000:2018; COSO ERM 2017.

⁶² Guía GIR V7.

⁶³ Guía DAFP V7.

⁶⁴ Política de Gobierno Digital; MSPI.

⁶⁵ Decreto 1122 de 2024 y Guía GIR V7.

⁶⁶ ISO 37001; Política Institucional Antisoborno.

⁶⁷ Ley 2195 de 2022; ISO 37001.

⁶⁸ COSO ERM 2017; Guía DAFP V7.

⁶⁹ Guía GIR V7.

⁷⁰ Guía GIR V7.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 13 de 64
---	---	--

Valor Público: Beneficios tangibles e intangibles generados por la gestión institucional para la ciudadanía y grupos de valor⁷¹.

Vulnerabilidad: Debilidad de un activo, proceso o control que puede ser explotada por una amenaza⁷².

5. Marco normativo

La presente Política de Gestión Integral del Riesgo se fundamenta en el marco constitucional, legal, reglamentario y técnico que orienta la gestión pública, el control interno, la transparencia, la integridad pública, la administración de riesgos, la seguridad de la información y la seguridad digital en las entidades del Estado. Estas disposiciones constituyen el referente para la implementación, mantenimiento, seguimiento y mejora continua de la Gestión Integral del Riesgo en la Justicia Penal Militar y Policial (JPMP).

Tipo de norma	Número	Año	Descripción - Epígrafe
Constitución Política	N/A	1991	Establece los principios de la función administrativa y la responsabilidad de las entidades públicas en el cumplimiento de los fines esenciales del Estado.
Ley	87	1993	<i>"Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado".</i>
Ley	489	1998	<i>"Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional".</i>
Ley	610	2000	<i>"Por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías".</i>
Ley	1474	2011	Estatuto Anticorrupción. Fortalece los mecanismos de prevención, investigación y sanción de actos de corrupción.
Ley	1712	2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
Decreto Ley	403	2020	Fortalece el control fiscal y la identificación de riesgos fiscales.
Ley	2195	2022	Adopta medidas en materia de transparencia, prevención y lucha contra la corrupción e incorpora mecanismos de integridad pública.

⁷¹ MIPG – Guía GIR V7.

⁷² MSPI y Guía GIR V7.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 14 de 64
---	---	--

Tipo de norma	Número	Año	Descripción - Epígrafe
Decreto	1083	2015	Decreto Único Reglamentario del Sector Función Pública.
Decreto	1499	2017	Actualiza el Modelo Integrado de Planeación y Gestión (MIPG).
Decreto	1122	2024	Reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por la Ley 2195 de 2022, en relación con los Programas de Transparencia y Ética Pública (PTEP).
Resolución	1519	2020	Define los estándares y directrices para publicar información conforme a la Ley de Transparencia y Acceso a la Información Pública.
CONPES	4070	2021	Política Nacional para el Control Interno y fortalecimiento institucional.
Política Nacional	N/A	Vigente	Política de Gobierno Digital. Establece lineamientos para la seguridad digital, transformación digital y gestión de riesgos tecnológicos.
Modelo	N/A	Vigente	Modelo de Seguridad y Privacidad de la Información (MSPI). Define lineamientos para la gestión de riesgos de seguridad de la información.
Programa	N/A	Vigente	Programa de Transparencia y Ética Pública (PTEP). Instrumento para la gestión de riesgos de corrupción, integridad pública y transparencia.
Guía Técnica DAFP	Versión 7	2025	Guía para la Gestión Integral del Riesgo en Entidades Públicas.
Marco Internacional	COSO ERM	2017	Enterprise Risk Management – Integrating with Strategy and Performance. Marco de referencia para la gestión integral del riesgo orientada a la generación y protección de valor público.
Norma Técnica Internacional	ISO 31000	2018	Directrices para la gestión del riesgo aplicables a cualquier tipo de organización.
Norma Técnica Internacional	ISO/IEC 27001	2022	Sistema de Gestión de Seguridad de la Información.
Norma Técnica Internacional	ISO 37001	2025	Sistemas de Gestión Antisoborno. Requisitos con orientación para su uso.

Fuente: Elaborado con fundamento en la Constitución Política de Colombia, la Ley 87 de 1993, el Decreto 1499 de 2017 y la *Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025)* del Departamento Administrativo de la Función Pública (DAFP).

La presente Política de Gestión Integral del Riesgo se implementará de manera articulada con la Política de Integridad Institucional, la Política de Lucha contra la

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 15 de 64
---	---	--

Corrupción y Antisoborno, el Programa de Transparencia y Ética Pública (PTEP), el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), la Política de Seguridad Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI), el Plan Estratégico de Tecnologías de la Información (PETI) y los demás instrumentos institucionales que contribuyan al fortalecimiento de la gestión del riesgo y del Sistema de Control Interno.

6. Roles y responsabilidades.

6.1 Gobierno del Riesgo

La Justicia Penal Militar y Policial adopta un modelo de Gobierno del Riesgo orientado a garantizar la integración de la Gestión Integral del Riesgo con la estrategia institucional, la planeación, la gestión, la toma de decisiones, el Sistema de Control Interno y la generación de valor público.

La Alta Dirección reconoce la Gestión Integral del Riesgo como un componente estratégico para el cumplimiento de los objetivos institucionales, la protección de los recursos públicos, el fortalecimiento de la integridad pública y el mejoramiento continuo del desempeño institucional. En consecuencia, promoverá una cultura organizacional fundamentada en la prevención, la transparencia, la integridad, el autocontrol, la responsabilidad y la mejora continua, asegurando que la gestión del riesgo se incorpore transversalmente en todos los procesos, proyectos, planes y actividades de la Entidad.

El Gobierno del Riesgo comprende el conjunto de estructuras de dirección, responsabilidades, mecanismos de supervisión, seguimiento y toma de decisiones mediante los cuales la Alta Dirección orienta, dirige y evalúa la efectividad de la Gestión Integral del Riesgo, garantizando su alineación con los objetivos institucionales, el marco normativo aplicable y las políticas de gestión y desempeño institucional. Para tal fin, ejercerá la supervisión estratégica mediante el esquema de Línea Estratégica, Primera, Segunda y Tercera Línea de Defensa, asegurando la definición y revisión periódica de la capacidad, el apetito y la tolerancia al riesgo, así como el seguimiento a la efectividad de los controles, los indicadores clave de riesgo (KRI), los planes de tratamiento y las acciones de mejora.

Asimismo, la Alta Dirección garantizará la disponibilidad de los recursos necesarios para la implementación, seguimiento, evaluación y mejora continua de la Gestión Integral del Riesgo, promoverá el fortalecimiento de las capacidades institucionales para la gestión de los riesgos y realizará seguimiento periódico a la aplicación de la presente política, impulsando su actualización cuando se presenten cambios

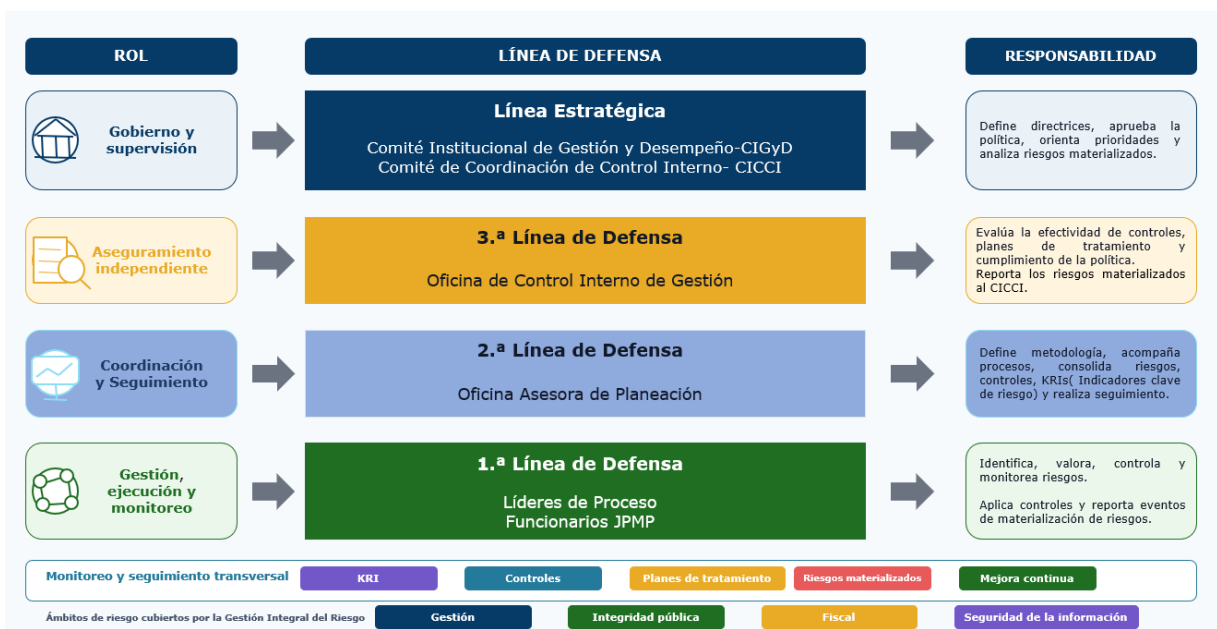
estratégicos, normativos, tecnológicos, operativos o del entorno que puedan afectar la exposición al riesgo de la Entidad.

En el marco de este modelo de gobierno, mantiene su compromiso con la prevención, detección, monitoreo y tratamiento de los riesgos de gestión, integridad pública, corrupción, fraude, conflictos de interés, riesgos fiscales, seguridad de la información, seguridad digital y demás riesgos que puedan afectar el cumplimiento de los objetivos institucionales, en articulación con el Programa de Transparencia y Ética Pública (PTEP), el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), el Modelo Integrado de Planeación y Gestión (MIPG) y el Sistema de Control Interno.

Finalmente, el Gobierno del Riesgo promoverá la responsabilidad compartida, la transparencia, la rendición de cuentas y la toma de decisiones basada en información confiable, oportuna y suficiente para fortalecer la gestión institucional y la generación de valor público.

La gestión del riesgo se desarrollará bajo el esquema de Líneas de Defensa, promoviendo una adecuada segregación de responsabilidades, el fortalecimiento del Gobierno del Riesgo y la coordinación entre las diferentes dependencias de la entidad tal como se presenta en la siguiente figura:

Figura 1. Responsabilidades por líneas de defensa



Fuente: Elaboración propia – Oficina Asesora de Planeación. Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Pública V.7.

6.2 Roles y responsabilidades

De conformidad con el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo Estándar de Control Interno –MECI y la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7, la entidad adopta el esquema de asignación de responsabilidades y roles que se distribuye en cuatro (4) líneas de la siguiente manera:

Tabla 1. Roles y responsabilidades para la implementación de la Política de Gestión Integral de Riesgos bajo el esquema de Líneas de Defensa.

Línea de defensa	Responsable	Rol	Responsabilidad
Línea Estratégica	Comité Institucional de Coordinación de Control Interno (CICCI)	Gobernanza y Supervisión	- Aprobar y realizar seguimiento a la Política de Gestión Integral del Riesgo. - Analizar riesgos estratégicos y fortalecer el Sistema de Control Interno. - Evaluar periódicamente los riesgos estratégicos y los riesgos emergentes que puedan afectar el cumplimiento de los objetivos institucionales. - Emitir recomendaciones de mejoras a la Política de Gestión Integral de Riesgos de la entidad.
	Comité Institucional de Gestión y desempeño	Supervisor	- Orientar la gestión del riesgo y su articulación con los objetivos institucionales. - Promover la asignación de recursos para la gestión de riesgos críticos. - Emitir recomendaciones de mejoras a la Política de Gestión Integral de Riesgos de la entidad.
Tercera Línea de Defensa	Oficina de Control Interno de Gestión	Aseguramiento independiente	- Brindar asesoría independiente en materia de riesgos y controles, sin asumir responsabilidades de gestión ni participar directamente en su identificación, diseño o implementación. - Evaluar de manera independiente la efectividad de la gestión integral del riesgo y de los controles implementados. - Verificar el cumplimiento de la política y de los planes de tratamiento. - Formular recomendaciones de mejora para fortalecer el Sistema de Control Interno y la gestión del riesgo. - Informar a la Alta Dirección sobre los resultados de sus evaluaciones. - Verificar la efectividad del esquema de líneas. - Verificar la implementación, monitoreo y seguimiento de los riesgos por parte de la primera y segunda línea de defensa.
Segunda Línea de Defensa	Oficina Asesora de Planeación	Coordinación y seguimiento	Formular y actualizar la metodología y los lineamientos para la gestión integral del riesgo.

Línea de defensa	Responsable	Rol	Responsabilidad
			- Asesorar y acompañar a los procesos en la identificación, valoración y tratamiento de riesgos. - Consolidar y administrar el Mapa de Riesgos Institucional, identificar riesgos emergentes y recomendar acciones de fortalecimiento de la Gestión Integral del Riesgo. - Consolidar y hacer seguimiento a la implementación de la política y al mapa institucional, y presentar información para la toma de decisiones. - Asesorar a la 1ª línea de defensa en temas clave para el Sistema de Control Interno: i) riesgos y controles; ii) planes de mejoramiento; iii) indicadores de gestión; iv) procesos y procedimientos.
Primera Línea de Defensa	Líderes de proceso (jefes, coordinadores u otro cargo) Funcionarios JPMP	Gestión, ejecución y monitoreo	- Identificar, analizar, valorar, controlar y monitorear los riesgos asociados a sus procesos o actividades, incluyendo riesgos emergentes derivados de cambios normativos, tecnológicos, operativos, sociales o del entorno institucional. - Implementar y mantener controles y acciones de tratamiento. - Reportar oportunamente riesgos materializados y eventos relevantes. - Mantener actualizada la información de riesgos y ejecutar acciones de mejora cuando corresponda. - Proponer las actualizaciones al Mapa de Riesgos resultantes de las autoevaluaciones del proceso. - Establecer planes de mejoramiento necesarios. - Informar a la Oficina Asesora de Planeación (segunda línea) sobre los riesgos materializados.

Fuente: Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (DAFP, 2025), el Modelo Integrado de Planeación y Gestión (MIPG) y el Modelo Estándar de Control Interno (MECI).

7. Análisis de contexto (interno y externo)

La gestión integral del riesgo debe partir de una comprensión adecuada del contexto en el que desarrolla su misión institucional. En consecuencia, la entidad realiza el análisis sistemático de los factores externos e internos que pueden incidir en el cumplimiento de sus objetivos estratégicos, la prestación del servicio de administración de justicia, el desempeño institucional y la generación de valor público.

Este análisis se realiza en la entidad con periodicidad anual, ejercicios en los que participan la alta dirección, los líderes de proceso y de dependencias, espacios que

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 19 de 64
---	---	---

permiten identificar condiciones, tendencias, cambios y eventos que puedan generar riesgos u oportunidades, constituyéndose en un insumo fundamental para la identificación, valoración, tratamiento, monitoreo y seguimiento de los riesgos, así como para la definición de la capacidad, el apetito y la tolerancia al riesgo institucional. Para tal fin, se consideran los factores del entorno interno y externo como son: político, económico, social, tecnológico, ambiental, legal y de comunicación, los cuales orientan la toma de decisiones y fortalecen la capacidad institucional para anticipar y gestionar los efectos derivados de la incertidumbre.

A continuación, se presentan los factores externos e internos, con los aspectos institucionales relevantes que deben ser considerados en el proceso de identificación y análisis de riesgos de la entidad.

Tabla 2. Factores externos de riesgo

Factor	Subfactor	Descripción
Político	Cambio de Gobierno o administración	1. Impacto del cambio de gobierno y las modificaciones de las Políticas Públicas (empleo, presupuesto, etc.) en la gestión institucional de la Entidad.
	Conflictos internos (nacionales) o externos (internacionales)	2. Conflictos nacionales e internacionales que actualmente se presentan a nivel nacional e internacional.
	Relacionamiento Institucional	3. Relacionamiento Institucional de la Entidad para el fortalecimiento de la Jurisdicción.
	Tratados Internacionales	4. Afectación de tratados internacionales sobre la función de la misionalidad de la Entidad.
Comunicación Interna/ Externa	Visibilidad de Entidad	1. Reconocimiento de la Entidad a nivel nacional e internacional
	Canales de comunicación oficiales de la Entidad	2. Actualización y uso de los canales y medios de comunicación para la difusión de la gestión realizada por la Entidad
	Atención a los grupos de interés	3. Estrategias de comunicación para la atención a los grupos de valor e interés de acuerdo con sus expectativas
Económico	Crisis económica del país	1. La situación económica en Colombia y a nivel mundial, así como las diferentes reformas económicas adoptadas por el Gobierno nacional
	Ajustes o modificaciones en temas tributarios	2. Incidencia de las normas tributarias y modificaciones presupuestales en el funcionamiento de la Entidad

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 20 de 64
---	---	--

Factor	Subfactor	Descripción
	PIB- Inflación	3. Afectación de la variación del PIB y la inflación en la planeación presupuestal de la Entidad
Tecnológico	Interoperabilidad de los sistemas de información del gobierno	1. Contribución de la interoperabilidad de los sistemas de información del gobierno al cumplimiento de la misionalidad de la Entidad
	Seguridad de la Información	2. Políticas para la ciber seguridad de la información
	Investigación, Promoción y desarrollo tecnológico	3. Desarrollo o participación en programas o proyectos tecnológicos institucionales o sectoriales para el funcionamiento y fortalecimiento de la Entidad
	Acceso a datos abiertos y fuentes de información de relevancia institucional.	4. Conocimiento de portales que contengan información pública y accesible y de interés para el desempeño de las funciones institucionales.
Ecológico y ambientales	Cambios Normativos	1. Cambios normativos en materia ambiental (Cambio climático, medición de huella de carbono)
	Riesgos Naturales	2. Los riesgos naturales (desastres, pandemias) y su impacto a nivel nacional (sede central y despachos) en el desarrollo de sus actividades
Social	Demografía	1. Influencia de los cambios demográficos y la movilidad social en Colombia sobre la administración de la Justicia Penal Militar y Policial
	Percepción Ciudadana	2. Conocimiento de la Entidad y percepción ciudadana sobre los resultados de gestión
	Patrones culturales	3. Patrones culturales y su afectación a la misionalidad de la Entidad
	Quejas y reclamos de grupos de interés por los aspectos o impactos que genera la Entidad.	4. Afectación de las quejas y reclamos de grupos de interés en el desarrollo de la misionalidad de la Entidad
Legal	Legislación sobre derechos humanos	1. Incidencia de la normatividad nacional en derechos humanos y en derecho internacional en la práctica administrativa y judicial
	Normatividad aplicable a los temas de Justicia Penal Militar y Policial	2. La normatividad y reglamentación nacional aplicable a los temas de Justicia Penal Militar y Policial
	Evaluaciones de organismos de control	1. Los planes de mejoramiento derivados de las auditorías de organismos de control.

Fuente: Elaboración propia, Oficina Asesora de Planeación. Análisis realizado mediante la metodología PESTEL, utilizada para identificar y evaluar factores políticos, económicos, sociales, tecnológicos, ambientales y legales que pueden incidir en la gestión institucional y en la exposición al riesgo entidad.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 21 de 64
---	---	--

Tabla 3. Factores internos de riesgo

Factor	Subfactor	Descripción institucional	Descriptorios o situaciones orientadoras
Direccionamiento estratégico	Plataforma estratégica	Coherencia y alineación de la misión, visión, objetivos estratégicos, planes, programas y proyectos institucionales con las necesidades de la jurisdicción.	Objetivos insuficientemente definidos; desarticulación entre estrategia y operación; cambios de prioridades; metas no alineadas; decisiones sin información suficiente; insuficiente evaluación de alternativas estratégicas.
Direccionamiento estratégico	Planeación institucional	Formulación, articulación, ejecución y seguimiento de los instrumentos de planeación institucional y sectorial.	Programación inadecuada; metas no medibles; recursos insuficientes; debilidades en el seguimiento; incumplimiento de cronogramas; falta de articulación entre planes, programas y proyectos.
Gobierno y gestión institucional	Gobierno del riesgo y toma de decisiones	Oportunidad y efectividad de las estructuras de dirección, supervisión, coordinación, rendición de cuentas y toma de decisiones.	Decisiones inoportunas; información insuficiente; ausencia de escalamiento; responsabilidades no definidas; supervisión limitada; falta de seguimiento a decisiones; concentración de decisiones.
Gobierno y gestión institucional	Líneas de defensa	Funcionamiento articulado de la Línea Estratégica y de la primera, segunda y tercera línea para gestionar, monitorear y evaluar los riesgos.	Duplicidad de funciones; ausencia de segregación; responsabilidades no definidas; deficiencias en el reporte; limitada coordinación; participación de la tercera línea en actividades de gestión; falta de seguimiento.
Gestión de procesos	Ejecución y administración de procesos	Condiciones relacionadas con el diseño, documentación, ejecución, coordinación y supervisión de procesos, procedimientos y actividades institucionales.	Falta de aplicación de procedimientos; actividades no documentadas; errores de registro, cálculo, revisión o autorización; ausencia de segregación; reprocesos; fallas de coordinación; supervisión insuficiente.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 22 de 64
---	---	---

Factor	Subfactor	Descripción institucional	Descriptorios o situaciones orientadoras
Gestión de procesos	Eficiencia operativa	Capacidad de los procesos para generar productos, servicios y resultados oportunos, pertinentes y de calidad.	Demoras; acumulación de trámites; incumplimiento de términos; duplicidad de actividades; errores recurrentes; baja capacidad operativa; cuellos de botella; pérdida de trazabilidad.
Gestión de procesos	Controles internos	Diseño, documentación, ejecución y efectividad de los controles establecidos para prevenir, detectar o corregir los riesgos.	Controles inexistentes o desactualizados; controles sin responsable; ejecución inoportuna; falta de evidencia; fuentes de información no confiables; ausencia de acciones ante desviaciones; controles manuales susceptibles de error.
Gestión de procesos	Mejora continua	Implementación de acciones correctivas, preventivas y de mejora derivadas del seguimiento, las auditorías, las materializaciones y las lecciones aprendidas.	Acciones vencidas; análisis de causas insuficiente; reincidencia de eventos; cierres sin evidencia; falta de evaluación de efectividad; ausencia de actualización del mapa de riesgos.
Talento humano	Capacidad y suficiencia de Funcionarios	Disponibilidad de personal, competencias, conocimientos y experiencia requeridos para cumplir los objetivos institucionales y de los procesos.	Insuficiencia de funcionarios; sobrecarga laboral; alta rotación; vacantes; ausencia de perfiles adecuados; pérdida de conocimiento; concentración de funciones críticas.
Talento humano	Competencias y capacitación	Desarrollo y actualización de conocimientos, habilidades y capacidades requeridas para el ejercicio de las funciones.	Falta de inducción o reinducción; capacitación insuficiente; desconocimiento de procedimientos; errores humanos; habilidades tecnológicas limitadas; desactualización normativa.
Talento humano	Conducta e integridad	Comportamientos de servidores y contratistas que pueden afectar el cumplimiento, la ética, la transparencia y la integridad institucional.	Incumplimiento de deberes; abuso de funciones; acceso indebido a información; ocultamiento de hechos; omisión de controles; conductas contrarias al Código de Integridad.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 23 de 64
---	---	--

Factor	Subfactor	Descripción institucional	Descriptorios o situaciones orientadoras
Talento humano	Gestión del conocimiento	Preservación, transferencia, apropiación y disponibilidad del conocimiento institucional.	Empalmes incompletos; conocimiento concentrado; pérdida de memoria institucional; inexistencia de repositorios; documentación insuficiente; falta de transferencia antes del retiro o cambio de personal.
Gestión financiera y presupuestal	Programación y asignación de recursos	Disponibilidad y suficiencia de recursos financieros para cumplir los objetivos, planes, programas y proyectos institucionales.	Programación inadecuada; insuficiencia presupuestal; recursos bloqueados; distribución no priorizada; falta de oportunidad en la asignación; diferencias entre necesidades y apropiaciones.
Gestión financiera y presupuestal	Ejecución y control financiero	Programación, ejecución, registro, conciliación y seguimiento de las operaciones presupuestales, contables y de tesorería.	Baja ejecución; errores contables o presupuestales; pagos indebidos; registros duplicados; cuentas sin conciliar; obligaciones sin soporte; demoras en pagos; incumplimiento del programa anual de caja.
Gestión financiera y presupuestal	Gestión fiscal	Manejo, administración, custodia, adquisición, disposición y control de bienes, recursos e intereses patrimoniales públicos.	Pérdida o deterioro de bienes; pagos sin cumplimiento de requisitos; manejo inadecuado de inventarios; falta de supervisión; decisiones que puedan ocasionar daño patrimonial; debilidades de custodia.
Tecnología e información	Sistemas de información	Disponibilidad, capacidad, confiabilidad, integración e interoperabilidad de los sistemas que soportan la gestión institucional.	Indisponibilidad de aplicaciones; obsolescencia; fallas de interoperabilidad; errores de configuración; capacidad insuficiente; dependencia de procesos manuales; soporte técnico inoportuno.
Tecnología e información	Seguridad de la información y ciberseguridad	Protección de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y de los servicios digitales.	Accesos no autorizados; pérdida o alteración de información; credenciales comprometidas; malware; phishing; vulnerabilidades; copias de respaldo insuficientes; incidentes sin gestión oportuna.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 24 de 64
---	---	--

Factor	Subfactor	Descripción institucional	Descriptorios o situaciones orientadoras
Tecnología e información	Calidad e integridad de datos	Exactitud, completitud, consistencia, actualización y disponibilidad de los datos utilizados para la operación y la toma de decisiones.	Datos incompletos; registros duplicados; información desactualizada; diferencias entre sistemas; captura errónea; ausencia de validaciones; fuentes no confiables.
Tecnología e información	Transformación digital	Implementación y sostenibilidad de iniciativas tecnológicas orientadas a mejorar la gestión y la prestación de servicios.	Proyectos tecnológicos sin sostenibilidad; resistencia al cambio; soluciones sin integración; limitaciones de infraestructura; automatización insuficiente; dependencia de contratistas.
Gestión documental y del conocimiento	Gestión documental	Producción, organización, clasificación, custodia, consulta y disposición de documentos y expedientes institucionales.	Expedientes incompletos; pérdida documental; versiones no controladas; archivo inadecuado; incumplimiento de tablas de retención; dificultades de consulta; documentos sin trazabilidad.
Gestión documental y del conocimiento	Información judicial y administrativa	Disponibilidad, integridad, reserva, autenticidad y conservación de la información generada en los procesos misionales y administrativos.	Pérdida de expedientes; acceso indebido; modificación no autorizada; información fragmentada; incumplimiento de reserva; fallas en la cadena de custodia documental.
Integridad y transparencia	Fraude interno	Posibilidad de actuaciones intencionales realizadas desde el interior de la entidad para obtener beneficios indebidos o generar afectaciones institucionales.	Manipulación de información; apropiación de recursos; alteración de registros; ocultamiento; abuso de acceso; uso indebido de bienes; acuerdos entre servidores o contratistas.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 25 de 64
---	---	--

Factor	Subfactor	Descripción institucional	Descriptorios o situaciones orientadoras
Integridad y transparencia	Fraude externo	Posibilidad de actuaciones intencionales de personas externas dirigidas a engañar a la entidad u obtener beneficios indebidos.	Documentos falsos; suplantación; reclamaciones fraudulentas; ataques informáticos; engaño; proveedores ficticios; apropiación de información; colusión con personal interno.
Integridad y transparencia	Soborno	Condiciones que pueden facilitar el ofrecimiento, promesa, entrega, solicitud o aceptación de ventajas indebidas para influir en decisiones o actuaciones institucionales.	Contactos sin trazabilidad; ofrecimiento de regalos o favores; intermediarios; decisiones discrecionales sin soporte; presión sobre responsables; ausencia de segregación.
Integridad y transparencia	Gestión inadecuada de conflictos de interés	Condiciones que pueden afectar la imparcialidad y objetividad por la existencia de intereses privados reales, potenciales o aparentes.	Falta de declaración; omisión de impedimentos; intervención en asuntos de interés particular; relaciones no reveladas; ausencia de análisis o seguimiento; gestión inoportuna del conflicto.
Integridad y transparencia	Corrupción interna o externa	Condiciones que pueden facilitar el uso indebido del poder, la función pública o los recursos para obtener beneficios particulares.	Manipulación de trámites; favorecimiento; presiones externas; acuerdos colusorios; información privilegiada; desviación de recursos; interferencia en decisiones; abuso de autoridad.
Integridad y transparencia	LA/FT/FP y conocimiento de terceros	Condiciones relacionadas con operaciones, relaciones o terceros que puedan exponer a la entidad a riesgos de lavado de activos, financiación del terrorismo o proliferación de armas.	Debida diligencia insuficiente; información incompleta de terceros; operaciones inusuales; contrapartes no verificadas; beneficiarios finales no identificados; señales de alerta no gestionadas.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 26 de 64
---	---	--

Factor	Subfactor	Descripción institucional	Descriptorios o situaciones orientadoras
Terceros y relaciones institucionales	Contratistas, proveedores y operadores	Riesgos derivados de las relaciones con personas naturales o jurídicas que suministran bienes, servicios o soluciones a la entidad.	Incumplimiento contractual; dependencia de proveedores/contratistas críticos; fallas de calidad; supervisión insuficiente; concentración de proveedores; información incompleta; conflictos de interés.
Terceros y relaciones institucionales	Convenios, alianzas y relaciones interinstitucionales	Condiciones derivadas de convenios, acuerdos, alianzas o actividades ejecutadas con otras entidades u organizaciones.	Responsabilidades ambiguas; información no compartida oportunamente; incumplimiento de compromisos; fallas de coordinación; ausencia de seguimiento; diferencias metodológicas.
Transacciones y operaciones	Trámites, decisiones y operaciones institucionales	Condiciones relacionadas con trámites, actuaciones, autorizaciones, movimientos de recursos y prestación de servicios a través de los canales institucionales.	Operaciones sin soporte; autorizaciones inadecuadas; duplicidad; alteración documental; suplantación; errores de registro; falta de validación; operaciones inusuales.
Infraestructura física y recursos	Instalaciones y equipamiento	Condiciones de las sedes, despachos, instalaciones, equipos y demás recursos físicos requeridos para la operación.	Deterioro; mantenimiento insuficiente; fallas de equipos; limitaciones de espacio; almacenamiento inadecuado; deficiencias de seguridad física; indisponibilidad de servicios públicos.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 27 de 64
---	---	--

Factor	Subfactor	Descripción institucional	Descriptorios o situaciones orientadoras
Infraestructura física y recursos	Bienes, inventarios y elementos institucionales	Administración, identificación, custodia, uso, traslado, mantenimiento y disposición de bienes institucionales.	Inventarios desactualizados; bienes sin identificación; pérdida; uso no autorizado; traslados sin soporte; elementos obsoletos; falta de mantenimiento; ausencia de responsables.
Continuidad de la operación	Continuidad de procesos y servicios	Capacidad institucional para mantener o restablecer las funciones y servicios esenciales ante situaciones disruptivas.	Ausencia de planes; indisponibilidad de funcionarios, sedes o sistemas; tiempos de recuperación no definidos; dependencia de personas o proveedores críticos; pruebas de continuidad insuficientes.
Eventos externos	Emergencias y alteraciones del entorno	Hechos externos que pueden afectar la operación y que no se encuentran bajo control directo de la entidad.	Desastres naturales; pandemias; alteraciones de orden público; ataques externos; interrupciones de servicios; restricciones de movilidad; eventos territoriales que afecten sedes o despachos.
Gestión ambiental	Uso de recursos y cumplimiento ambiental	Condiciones relacionadas con consumo de recursos, generación de residuos, impactos ambientales y cumplimiento de obligaciones ambientales.	Consumo ineficiente; manejo inadecuado de residuos; incumplimiento de requisitos; eventos climáticos; afectación de infraestructura; ausencia de medición o seguimiento ambiental.
Comunicación y reputación	Comunicación interna y externa	Gestión de información institucional dirigida a servidores, ciudadanía, grupos de valor, medios y demás partes interesadas.	Información inoportuna o inconsistente; canales desactualizados; publicaciones erróneas; falta de coordinación; respuesta tardía; divulgación no autorizada; mensajes contradictorios.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 28 de 64
---	---	--

Factor	Subfactor	Descripción institucional	Descriptorios o situaciones orientadoras
Comunicación y reputación	Confianza y percepción institucional	Condiciones que pueden afectar la credibilidad, legitimidad, reconocimiento y confianza en la JPMP.	Quejas reiteradas; falta de transparencia; desinformación; atención inadecuada; incumplimiento de compromisos; manejo deficiente de crisis; afectación pública sostenida.
Cumplimiento normativo	Gestión jurídica y regulatoria	Identificación, interpretación, aplicación, actualización y seguimiento del marco normativo aplicable a la entidad y a sus procesos.	Desconocimiento normativo; interpretación inadecuada; incumplimiento de términos; procedimientos desactualizados; vacíos regulatorios; decisiones sin sustento; cambios normativos no implementados.

Fuente: Elaboración propia, Oficina Asesora de Planeación. Adaptado de los lineamientos sobre análisis de contexto interno y gestión integral del riesgo establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas V.7

Notas:

Nota 1. Los factores y descriptorios incluidos en la tabla son orientadores y no exhaustivos. Cada proceso podrá identificar factores adicionales de acuerdo con su naturaleza, objetivo, alcance, actividades críticas, productos, servicios, grupos de valor, recursos y condiciones particulares de operación.

Nota 2. Un riesgo podrá estar relacionado con uno o varios factores. Para efectos del registro en el Mapa Integral de Riesgos Institucional, deberá seleccionarse el factor principal y documentarse, cuando corresponda, los factores asociados.

Nota 3. La identificación del factor de riesgo no reemplaza el análisis de causas. El factor corresponde a una condición que incrementa la exposición; la causa inmediata corresponde a la circunstancia que facilita el evento; la causa raíz explica su origen fundamental; y la consecuencia corresponde a la afectación derivada de su materialización.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 29 de 64
---	---	----------------------------

8. Política de gestión integral del riesgo.

La Justicia Penal Militar y Policial reconoce la Gestión Integral del Riesgo como un componente estratégico de la gestión institucional y un elemento fundamental para el fortalecimiento de la gobernanza, la toma de decisiones, el control interno, la generación de valor público y el cumplimiento de los objetivos institucionales.

En este sentido, la entidad adopta un enfoque integral, preventivo y basado en riesgos que permita gestionar de manera sistemática los eventos que puedan afectar el logro de sus objetivos, la prestación de los servicios, la protección de los recursos públicos, la integridad institucional y la confianza de los grupos de valor.

La Gestión Integral del Riesgo se desarrollará de manera articulada con el Modelo Integrado de Planeación y Gestión (MIPG), el Sistema de Control Interno, el Programa de Transparencia y Ética Pública (PTEP), el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), la Política de Seguridad Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los demás instrumentos institucionales que contribuyan al fortalecimiento de la capacidad institucional para gestionar la incertidumbre y responder oportunamente a los riesgos y oportunidades del entorno.

Para el cumplimiento de esta política, la entidad adopta los siguientes lineamientos:

a. Integración con la gestión institucional

La Gestión Integral del Riesgo deberá incorporarse en la planeación, ejecución, seguimiento, evaluación y mejora de los procesos, planes, programas, proyectos y demás actividades institucionales, contribuyendo al cumplimiento de los objetivos estratégicos y misionales.

b. Gobierno del Riesgo

La Alta Dirección promoverá mecanismos de dirección, supervisión y rendición de cuentas que permitan asegurar la adecuada implementación, monitoreo y fortalecimiento de la Gestión Integral del Riesgo en todos los niveles de la Entidad.

c. Gestión de riesgos institucionales

La entidad identificará, analizará, evaluará, tratará, monitoreará y comunicará los riesgos que puedan afectar el cumplimiento de los objetivos

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 30 de 64
---	---	---

institucionales, considerando el contexto interno y externo, las interrelaciones entre procesos y los cambios que puedan generar riesgos emergentes.

d. Gestión de riesgos de corrupción e integridad pública

La entidad fortalecerá la prevención, detección y tratamiento de riesgos de corrupción e integridad pública mediante la articulación con el Programa de Transparencia y Ética Pública (PTEP), el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), la Política de Integridad y los demás mecanismos institucionales orientados a promover la transparencia, la ética pública y la lucha contra la corrupción.

e. Gestión de riesgos fiscales

La entidad gestionará los riesgos fiscales asociados a la administración de los recursos públicos, con el propósito de prevenir afectaciones al patrimonio público y fortalecer la eficiencia, eficacia, economía y transparencia de la gestión institucional.

f. Gestión de riesgos de seguridad de la información y seguridad digital

La entidad gestionará los riesgos asociados a la seguridad de la información, la seguridad digital y la ciberseguridad, garantizando la protección de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información institucional, en armonía con la Política de Seguridad Digital y el Modelo de Seguridad y Privacidad de la Información (MSPI).

g. Gestión basada en apetito y tolerancia al riesgo

Las decisiones relacionadas con el tratamiento y aceptación de riesgos se desarrollarán conforme a los niveles de capacidad, apetito y tolerancia al riesgo definidos por la Entidad, priorizando aquellos riesgos que puedan comprometer significativamente el cumplimiento de los objetivos institucionales, la legalidad, la integridad, la seguridad de la información o la protección de los recursos públicos.

h. Monitoreo, seguimiento y mejora continua

La Gestión Integral del Riesgo será objeto de monitoreo, seguimiento y evaluación permanente por parte de las líneas de defensa, con el fin de verificar la efectividad de los controles, la ejecución de los planes de

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 31 de 64
---	---	--

tratamiento, la evolución de los riesgos y la implementación de acciones orientadas al fortalecimiento institucional y la mejora continua.

i. Comunicación y toma de decisiones

La información relacionada con la gestión de riesgos deberá ser confiable, oportuna y accesible para las instancias responsables, facilitando la toma de decisiones basada en evidencia y el fortalecimiento de la cultura institucional de gestión del riesgo.

j. Gestión de oportunidades

La entidad promoverá la identificación y análisis de oportunidades derivadas del conocimiento del contexto institucional, la gestión de los riesgos, la innovación, la transformación digital y la mejora continua, con el fin de fortalecer el desempeño institucional, optimizar la utilización de los recursos, incrementar la capacidad de respuesta frente a los cambios del entorno y contribuir a la generación de valor público.

K. Responsabilidad de las Líneas de Defensa

La Gestión Integral del Riesgo se desarrollará bajo el esquema de líneas de defensa en consonancia con el MIPG, garantizando una participación coordinada y complementaria en la identificación, monitoreo, seguimiento, control y evaluación de los riesgos institucionales.

9. Apetito, tolerancia y capacidad de riesgo.

La Justicia Penal Militar y Policial adopta la capacidad de riesgo, el apetito al riesgo y la tolerancia al riesgo como criterios institucionales para orientar la gestión de los riesgos y apoyar la toma de decisiones relacionadas con su aceptación, tratamiento, monitoreo y seguimiento, en concordancia con los objetivos institucionales, el Modelo Integrado de Planeación y Gestión (MIPG) y el Sistema de Control Interno.

La capacidad de riesgo corresponde al nivel máximo de exposición que la entidad puede asumir sin comprometer el cumplimiento de su misión, la prestación del servicio, la sostenibilidad institucional o la protección de los recursos públicos.

El apetito al riesgo define el nivel de riesgo que la entidad está dispuesta a aceptar para alcanzar sus objetivos institucionales, mientras que **la tolerancia al**

riesgo establece las variaciones aceptables respecto de dicho nivel antes de requerir acciones adicionales de tratamiento.

Estos criterios se definen en los niveles de aceptación del riesgo y constituyen el marco de referencia para la valoración y gestión de los riesgos institucionales.

9.1 Criterios institucionales de aceptación del riesgo

Se gestionará los riesgos de acuerdo con los niveles de riesgo residual obtenidos en su valoración, aplicando medidas de monitoreo, fortalecimiento de controles o tratamiento, según corresponda.

Tabla 1. Criterios institucionales para la aceptación del riesgo

Nivel de riesgo residual	Tratamiento institucional
Bajo	Riesgo aceptable. Mantener controles y monitoreo periódico.
Moderado	Riesgo tolerable. Evaluar fortalecimiento de controles y seguimiento permanente.
Alto	Riesgo no deseable. Requiere acciones de tratamiento obligatorias.
Extremo	Riesgo no aceptable. Requiere intervención inmediata y seguimiento por las instancias competentes.

Fuente: Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025) e incorporando criterios institucionales de la Justicia Penal Militar y Policial.

9.2 Niveles de aceptación del riesgo

La Justicia Penal Militar y Policial establece los niveles de aceptación del riesgo con base en el apetito del riesgo institucional, la criticidad de los procesos y la naturaleza de cada tipología de riesgo, tomando como referencia la Guía para la Gestión Integral del Riesgo V7. La aceptación del riesgo residual deberá estar debidamente sustentada por el líder del proceso y contar con el acompañamiento metodológico de la Oficina Asesora de Planeación como segunda línea de defensa.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 33 de 64
---	---	---

a. Riesgos susceptibles de aceptación

Los riesgos de gestión, seguridad de la información, SST, ambientales y demás riesgos operativos podrán ser aceptados únicamente cuando, una vez evaluados los controles existentes y aplicadas las acciones de tratamiento correspondientes, su nivel de riesgo residual se ubique dentro del apetito de riesgo definido por la entidad y se evidencie la efectividad de los controles implementados.

Cuando el riesgo residual se ubique en zonas de riesgo alta o extrema, el líder del proceso deberá formular e implementar acciones adicionales de tratamiento orientadas a reducir su probabilidad o impacto, manteniendo seguimiento permanente a su evolución.

b. Riesgos no aceptables

La entidad no aceptará riesgos asociados con:

- Corrupción.
- Integridad pública.
- Fraude.
- Riesgo fiscal.
- Lavado de activos y financiación del terrorismo.
- Riesgos estratégicos que comprometan el cumplimiento de la misión institucional.
- Riesgos que afecten significativamente la prestación del servicio de administración de justicia penal militar y policial, el cumplimiento normativo o la protección de los derechos fundamentales.

Para estas tipologías, deberán adoptarse y mantenerse acciones de tratamiento, fortalecimiento y monitoreo permanente hasta reducir su exposición a niveles compatibles con los objetivos institucionales.

c. Monitoreo y Seguimiento

Todos los riesgos incluidos en el Mapa de Riesgos Institucional deberán ser objeto de monitoreo y seguimiento periódico por parte de los líderes de proceso, conforme a los lineamientos definidos por la entidad y a los ciclos de seguimiento institucional establecidos por la Oficina Asesora de Planeación.

Los líderes de proceso serán responsables de verificar la eficacia de los controles, reportar la materialización de riesgos, implementar las acciones de tratamiento y mantener actualizada la información registrada en los instrumentos institucionales de gestión del riesgo.

9.2.1 Estrategia para combatir el riesgo

Una vez realizado el análisis inicial del riesgo y verificando el nivel de este, se debe tomar la decisión de aceptar, reducir o evitar, de acuerdo con la decisión se identifica la necesidad de formular plan de tratamiento dentro del respectivo mapa de riesgos.

Tabla 4. Estrategias para combatir el riesgo

Estrategia	Descripción
Evitar	Eliminar la actividad, proceso o situación que origina el riesgo cuando su nivel de exposición resulte inaceptable o no pueda gestionarse adecuadamente mediante controles.
Reducir o mitigar	Implementar controles, planes de acción o medidas de tratamiento orientadas a disminuir la probabilidad de ocurrencia y/o el impacto del riesgo hasta niveles aceptables para la entidad.
Transferir o compartir	trasladar o distribuir parte de las consecuencias del riesgo a un tercero mediante mecanismos legalmente permitidos, tales como pólizas, contratos u otros instrumentos de protección.
Aceptar	Asumir el riesgo residual cuando, una vez valorado y aplicados los controles correspondientes, se encuentre dentro de los niveles de capacidad, apetito y tolerancia al riesgo definidos por la entidad

La selección de la estrategia de tratamiento deberá sustentarse en los resultados de la valoración del riesgo, la efectividad de los controles existentes, los criterios de capacidad, apetito y tolerancia al riesgo institucional, así como en un análisis de costo-beneficio que permita determinar la alternativa más adecuada para la protección de los objetivos institucionales.

9.3 Umbral del riesgo

Todos los riesgos identificados por la entidad deberán contar con un umbral definido y documentados en el Mapa de Riesgos Institucional, entendido como el nivel máximo de exposición al riesgo que la entidad está dispuesta a asumir en relación con el cumplimiento de sus objetivos estratégicos, el marco normativo aplicable y las directrices establecidas por la Alta Dirección. La definición de este umbral permite determinar el límite de tolerancia aceptable para cada riesgo y facilita el monitoreo de su comportamiento. Cuando un riesgo supere el umbral establecido, se considerará que ha excedido el nivel de aceptación definido por la entidad, por lo que deberán implementarse de manera oportuna acciones de

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 35 de 64
---	---	---

tratamiento, mitigación o correctivas que permitan reducir su impacto y probabilidad, llevándolo nuevamente a un rango tolerable.

9.4 Indicadores Clave de Proceso (KPI) e Indicadores Clave de Riesgo (KRI)

La entidad fortalecerá el monitoreo y la toma de decisiones mediante la articulación de los **Indicadores Clave de Proceso- KPI** y los **Indicadores Clave de Riesgo- KRI**. Los KPI permiten medir el desempeño, la eficiencia y el nivel de cumplimiento de los objetivos estratégicos, tácticos y operativos de los procesos, planes, programas y proyectos; mientras que los KRI constituyen mecanismos de alerta temprana que permiten identificar variaciones en la exposición al riesgo, riesgos emergentes y posibles condiciones que puedan afectar el logro de los objetivos institucionales.

La aplicación integrada de ambos tipos de indicadores permitirá no solo evaluar los resultados obtenidos, sino también anticipar situaciones que puedan comprometer la generación de valor público, la continuidad de la operación, el cumplimiento de las obligaciones legales y el logro de los objetivos institucionales. En consecuencia, los procesos deberán definir y mantener indicadores alineados con sus objetivos, riesgos, capacidad de riesgo, apetito y tolerancia al riesgo, garantizando su seguimiento periódico y la adopción oportuna de acciones preventivas, correctivas o de mejora cuando los resultados o las señales de riesgo superen los umbrales establecidos por la Entidad.

Lineamientos

- Los procesos deberán definir KPI para medir el desempeño y cumplimiento de sus objetivos.
- Los riesgos identificados deberán contar con al menos un KRI cuando su nivel de exposición, criticidad o impacto así lo requiera.
- Los KRI deberán incluir umbrales de seguimiento que permitan generar alertas tempranas y activar acciones de tratamiento.
- Los resultados de los KPI y KRI deberán analizarse de manera conjunta para fortalecer la toma de decisiones basada en evidencia.
- Los indicadores deberán ser objeto de seguimiento periódico y reportarse en los mecanismos institucionales definidos para el monitoreo de la gestión y de los riesgos.
- La Oficina Asesora de Planeación, como segunda línea de defensa, orientará la metodología para la definición, seguimiento y mejora de los KRI institucionales.

9.4.1 Alcance Indicadores KPI e KRI

Tabla 5. Alcance aplicación KPI y KRI

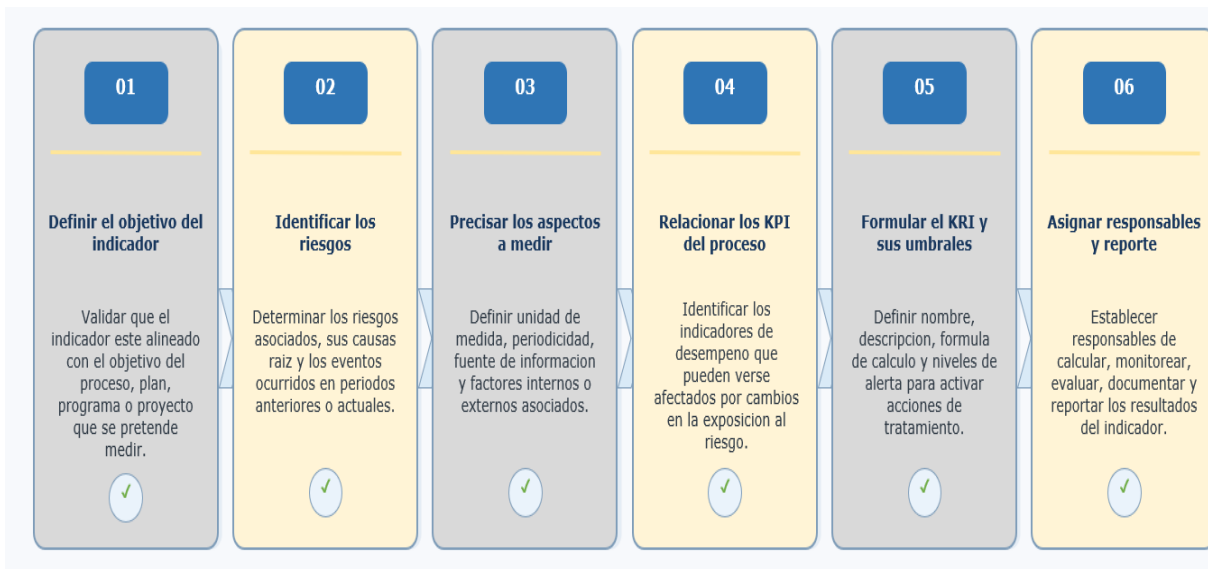
Indicadores Clave de Proceso (KPI)	Indicadores Clave de Riesgo (KRI)
Permiten medir periódicamente el desempeño general de la entidad y sus principales unidades operativas.	Complementan el seguimiento a los resultados de la entidad.
Tomando como referencia las metas establecidas, por procesos, unidades 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 de las acciones, logrando tomar decisiones con mayor certeza y confiabilidad.	Facilitan el proceso de generación de informes y el escalamiento de los riesgos.

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

9.4.2 Criterios para la formulación, seguimiento y monitoreo de los KRI.

Los Indicadores Clave de Riesgo (KRI) son métricas utilizadas para monitorear el comportamiento de variables asociadas a los riesgos identificados, proporcionando información oportuna sobre cambios en los niveles de exposición al riesgo y permitiendo la generación de alertas tempranas para la toma de decisiones. Asimismo, facilitan el seguimiento de tendencias, la evaluación de la efectividad de los controles y la implementación de acciones de tratamiento cuando se superen los umbrales definidos por la Entidad. Para su formulación, seguimiento y monitoreo, se deberán observar los siguientes criterios:

- a. Definición y construcción de los KRI**, para la formulación de estos indicadores se establecen los siguientes pasos:



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

Nota: Cada proceso podrá ajustar la periodicidad, fuente, umbral y responsable del KRI de acuerdo con la criticidad del riesgo y los lineamientos institucionales y a lo establecido en la Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025).

b. Umbrales de alerta y semaforización: Los KRI deberán contar con umbrales de seguimiento y mecanismos de semaforización que permitan identificar oportunamente cambios en los niveles de exposición al riesgo y facilitar la toma de decisiones.

Los líderes de proceso serán responsables de definir los valores de referencia, teniendo en cuenta la naturaleza del riesgo, los objetivos del proceso, plan, programa o proyecto y su relación con los Indicadores Clave de Desempeño (KPI). Como mínimo, los KRI deberán clasificarse en tres niveles: verde, cuando el comportamiento del riesgo se encuentre dentro de los rangos aceptables definidos por la Entidad; amarillo, cuando evidencie una tendencia de incremento que requiera seguimiento y análisis; y rojo, cuando supere los niveles de tolerancia o los umbrales establecidos, requiriendo la adopción inmediata de acciones de tratamiento.

Tabla 6. Umbrales de alerta y semaforización

Nivel	Estado	Interpretación	Acción esperada
Verde	Aceptable	El resultado del KRI se encuentra dentro de los rangos de exposición al riesgo aceptados por la Entidad y alineados con el apetito de riesgo definido.	Realizar seguimiento ordinario.
Amarillo	Alerta	El resultado del KRI evidencia una tendencia creciente o se aproxima al umbral de tolerancia establecido.	Intensificar el monitoreo y evaluar acciones preventivas.
Rojo	Crítico	El resultado del KRI supera el umbral de tolerancia o el apetito de riesgo definido por la Entidad.	Implementar acciones de tratamiento, mitigación o escalamiento, según corresponda.

Fuente: Elaboración propia – Oficina Asesora de Planeación. Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025) del Departamento Administrativo de la Función Pública (DAFP).

Nota: Los resultados de los KRI deberán analizarse en función de los umbrales definidos y del apetito de riesgo institucional. Los niveles amarillo y rojo requerirán acciones de seguimiento, prevención, mitigación o tratamiento, según corresponda.

- c. Relación del KRI con el apetito de riesgo:** El análisis de los resultados de los KRI deberá realizarse en concordancia con el apetito de riesgo institucional. Cuando el indicador se mantenga dentro de los niveles de exposición aceptados por la entidad, se entenderá que el riesgo se encuentra bajo control y dentro de los parámetros definidos por la Alta Dirección. Cuando el resultado se aproxime al umbral de alerta, deberán fortalecerse las actividades de monitoreo y evaluación para prevenir la materialización del riesgo. Si el indicador supera el nivel de tolerancia o el apetito de riesgo definido, el responsable deberá implementar y reportar las acciones preventivas, correctivas o de mitigación necesarias para retornar el riesgo a un nivel aceptable, tal como se señala a continuación:

Tabla 7. Relación del KRI con el apetito de riesgo

Resultado del KRI	Significado	Gestión requerida
Dentro del apetito de riesgo	La operación y el riesgo se mantienen dentro de lo que la Entidad está dispuesta a asumir frente a sus objetivos, el marco legal y las disposiciones de la Alta Dirección.	Mantener seguimiento ordinario.
Cercano al umbral de alerta	El riesgo presenta incremento y podría salir del rango tolerable si la tendencia continúa.	Reforzar monitoreo y definir acciones preventivas.
Excede el apetito de riesgo	El riesgo supera el umbral que la Entidad está dispuesta a asumir.	Adoptar acciones correctivas o de mitigación para retornar a un rango tolerable.

Fuente: Elaboración propia – Oficina Asesora de Planeación. Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025) del Departamento Administrativo de la Función Pública (DAFP).

- d. Responsables del KRI:** Para cada Indicador Clave de Riesgo (KRI) se deberán definir los responsables de calcular, monitorear, evaluar, documentar y reportar los resultados del indicador. Esta asignación deberá incluir la periodicidad de medición, la fuente de información, el mecanismo de reporte y las acciones que deberán activarse cuando el resultado se ubique en nivel de alerta o criticidad.

La Oficina Asesora de Planeación, en su rol de segunda línea de defensa, consolidará la información reportada por los procesos, analizará tendencias, identificará alertas tempranas, riesgos emergentes y desviaciones relevantes, y presentará los resultados a las instancias de seguimiento y toma de decisiones de la Entidad para la adopción de las acciones que correspondan.

- e. Reporte y monitoreo del KRI:** La entidad realizará el seguimiento periódico a los KPI y KRI con el fin de evaluar el desempeño de los procesos, identificar alertas tempranas y fortalecer la toma de decisiones. Los líderes de proceso serán responsables de su monitoreo y reporte, mientras que la Oficina Asesora de Planeación consolidará la información, analizará tendencias y desviaciones relevantes, y presentará los resultados a las instancias correspondientes para la definición de acciones de mejora, tratamiento o mitigación.

Tabla 8. Criterios para el reporte, monitoreo y escalamiento de los KRI.

Elemento	KPI	KRI	Criterio de escalamiento
Frecuencia mínima	Trimestral	Mensual o trimestral según criticidad	Desviación significativa frente a la meta o umbral
Responsable	Líder de proceso	Líder de proceso y gestor del riesgo	Superación del umbral o nivel de tolerancia
Análisis	Desempeño y resultados	Tendencia, exposición y alertas tempranas	Necesidad de tratamiento, mitigación o escalamiento

Fuente: Elaboración propia – Oficina Asesora de Planeación. Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025) del Departamento Administrativo de la Función Pública (DAFP).

9.5 Revisión y actualización

La Oficina Asesora de Planeación revisará periódicamente los criterios de capacidad, apetito y tolerancia al riesgo en coordinación con las instancias institucionales competentes, considerando cambios en el contexto estratégico, normativo, tecnológico, financiero y operativo de la Entidad.

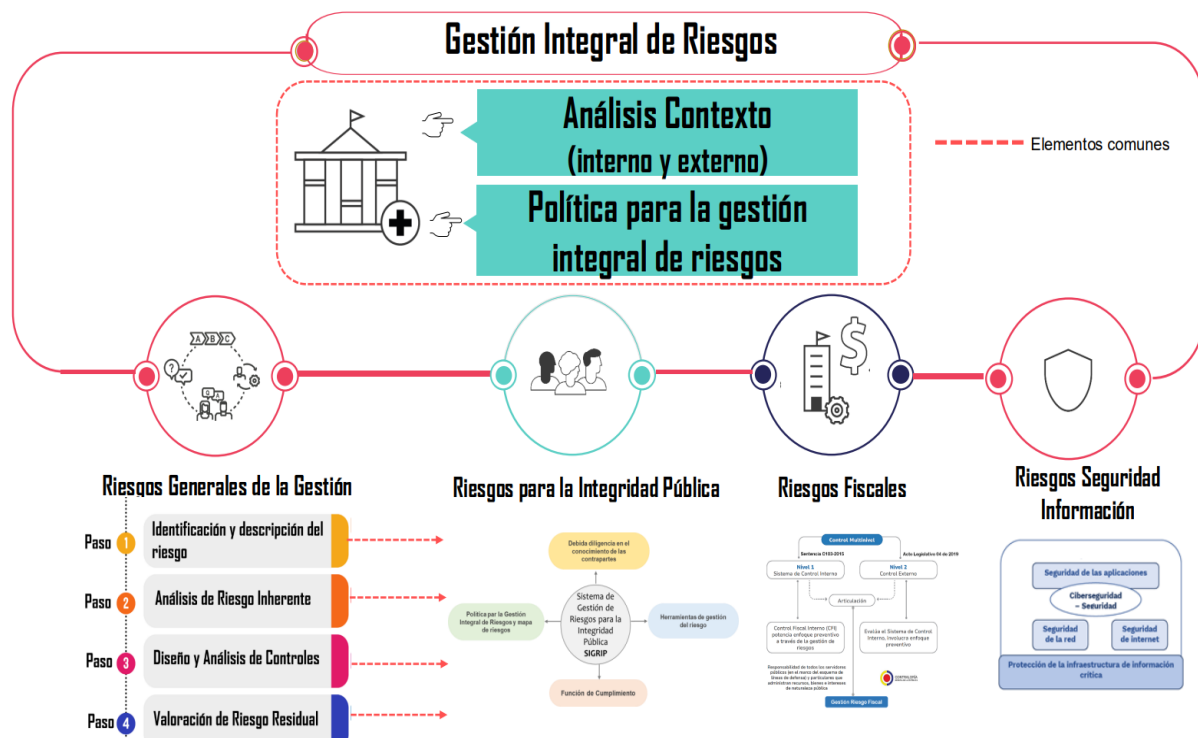
Su aplicación y desarrollo se realizarán a través de la Matriz Institucional de Riesgos de la JPMP, la cual hará parte de los anexos metodológicos de la presente política.

10. Metodología para la gestión integral del riesgo.

Con el fin de gestionar integralmente los riesgos que pueden afectar el cumplimiento de la misión y los objetivos institucionales de la JPMP, se articulan los riesgos asociados al patrimonio público, la seguridad de la información, la confianza en el entorno digital y la integridad en el ejercicio de la función pública. La **Figura 2** presenta esta articulación y los elementos comunes de la Gestión Integral del Riesgo, incluyendo el análisis del contexto interno y externo, la definición de la política y las etapas metodológicas de identificación, análisis, evaluación de controles y valoración del riesgo residual, aplicables a las diferentes tipologías de riesgo contempladas en la **Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 (2025)**, cuyos lineamientos

constituyen la base metodológica adoptada por la entidad para la administración integral de sus riesgos.

Figura 2. Articulación ámbitos para la gestión integral de riesgos



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

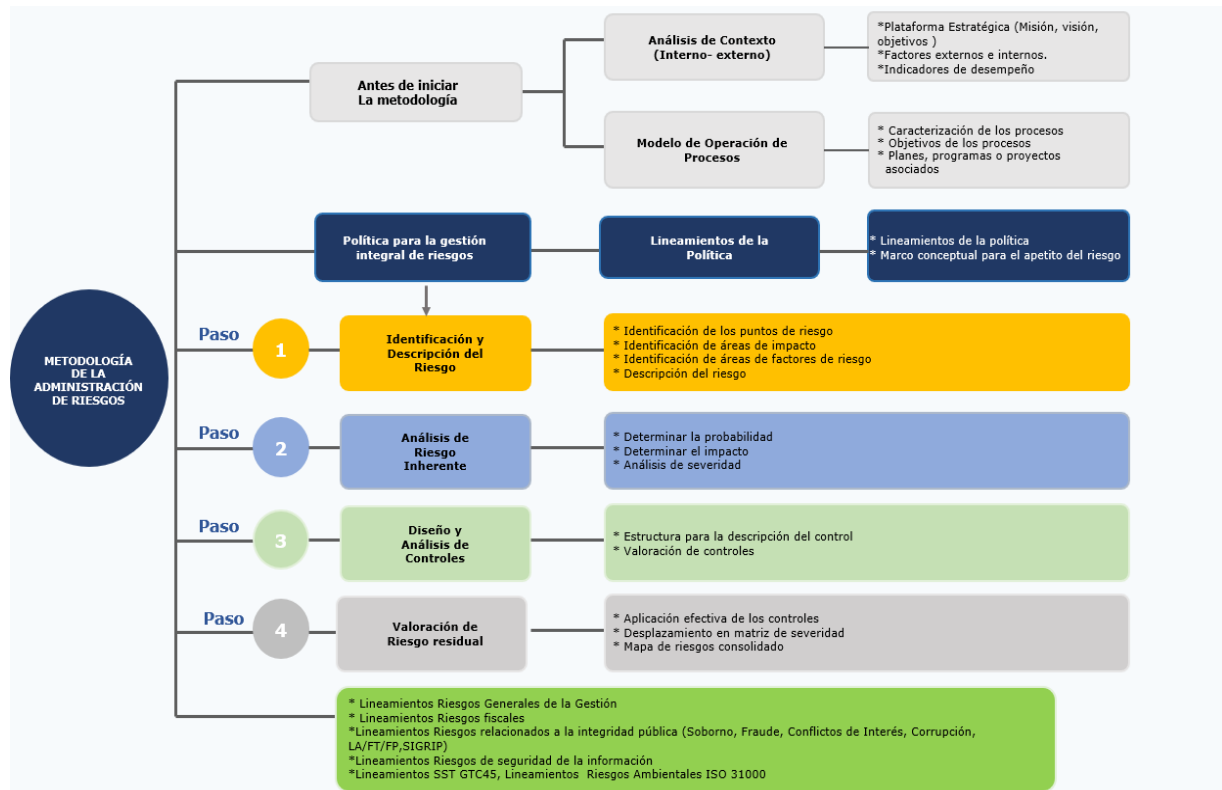
En consonancia con lo anterior, la Justicia Penal Militar y Policial adoptará la metodología para la Gestión Integral del Riesgo establecida por el Departamento Administrativo de la Función Pública (DAFP).

La aplicación de esta metodología se desarrollará de manera articulada con el Modelo Integrado de Planeación y Gestión (MIPG), el Sistema de Control Interno, el Programa de Transparencia y Ética Pública (PTEP), la Política de Seguridad Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los demás instrumentos institucionales aplicables.

En desarrollo de los lineamientos establecidos en la citada guía, la entidad implementará la metodología de Gestión Integral del Riesgo considerando su contexto institucional, su naturaleza jurídica y las particularidades propias de la

administración de justicia. Para tal efecto, la gestión de los riesgos institucionales se desarrollará a través de las siguientes pasos:

Figura 3. Metodología para la Gestión Integral del Riesgo



Fuente: Elaboración propia – Oficina Asesora de Planeación. Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025) del Departamento Administrativo de la Función Pública (DAFP).

10.1 Identificación y descripción del riesgo

En esta etapa se debe comprender el contexto estratégico, institucional y operativo de la Justicia Penal Militar y Policial, considerando los factores internos y externos que pueden incidir en el cumplimiento de los objetivos institucionales y de los procesos (ver numeral 7). Para ello, se tendrán en cuenta el análisis de contexto, el direccionamiento estratégico, la caracterización de los procesos, los procedimientos, los recursos disponibles, el marco normativo aplicable, las necesidades y expectativas de las partes interesadas y los resultados de ejercicios previos de seguimiento y evaluación.

La identificación de riesgos deberá realizarse a partir del análisis de los objetivos estratégicos, identificando los eventos que puedan afectar su cumplimiento, así

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 43 de 64
---	---	---

como sus posibles causas, consecuencias, puntos de riesgo y áreas de impacto. Este análisis deberá sustentarse en información histórica, lecciones aprendidas, resultados de auditorías, evaluaciones de control y demás fuentes de información relevantes para la gestión institucional.

Para los riesgos fiscales se deberán identificar los puntos de riesgo fiscal y las circunstancias inmediatas que puedan comprometer la adecuada administración y protección de los recursos públicos. En cuanto a los riesgos de seguridad de la información, se deberá considerar el inventario de activos de información asociado a cada proceso, así como las amenazas y vulnerabilidades que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

Asimismo, la identificación de riesgos deberá incorporar las necesidades y expectativas de los usuarios, ciudadanos, servidores públicos y demás grupos de valor, con el fin de reconocer situaciones que puedan afectar la prestación de los servicios, la administración de justicia, la transparencia institucional, la continuidad de la operación y el logro de los objetivos estratégicos de la entidad.

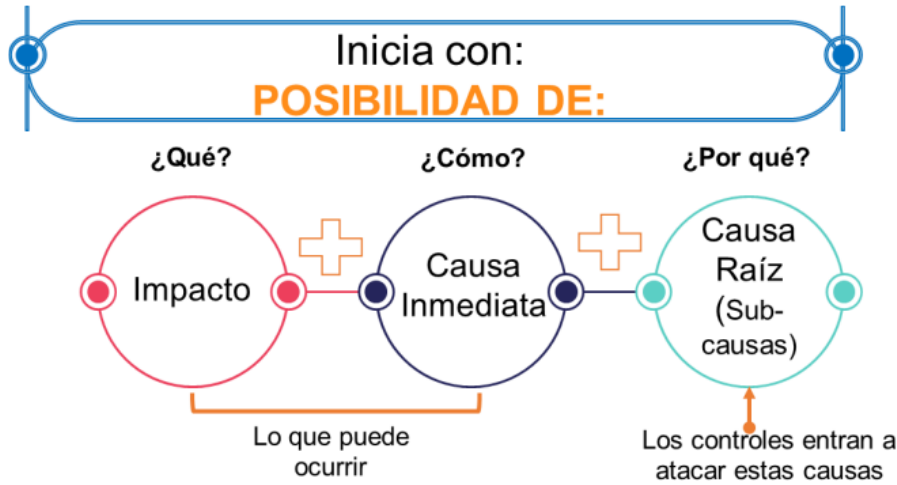
En desarrollo de este ejercicio, la Oficina Asesora de Planeación, como instancia de segunda línea de defensa, brindará asesoría y acompañamiento metodológico a los líderes de proceso, responsables de la primera línea de defensa, mediante mesas de trabajo y espacios de orientación técnica, con el propósito de asegurar la correcta aplicación de la metodología de administración del riesgo adoptada por la JPMP y la adecuada identificación de riesgos de gestión, corrupción, fiscales, seguridad de la información y demás riesgos aplicables a la Entidad.

10.1.1 Descripción del riesgo

Los riesgos identificados deberán describirse de manera clara, objetiva y verificable, estableciendo la relación entre sus causas, el evento de riesgo y sus posibles consecuencias.

Así mismo, se analizarán los factores que inciden en su materialización, la efectividad de los controles existentes y el nivel de exposición al riesgo, con el fin de facilitar su posterior valoración y tratamiento.

Figura 3. Estructura para la descripción del riesgo



Fuente: Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025).

Con el fin de asegurar una identificación y descripción adecuada de los riesgos, se deberá realizar un análisis que permita determinar qué puede ocurrir, por qué puede ocurrir y cuáles serían sus posibles consecuencias para la entidad. Este ejercicio debe diferenciar claramente las causas inmediatas de las causas raíz, identificar las condiciones que favorecen la materialización del riesgo y establecer los impactos potenciales sobre el cumplimiento de los objetivos institucionales. Para ello, se deberán considerar los siguientes elementos:

Tabla 9. Elementos descripción del riesgo

Elemento	Punto clave
Impacto (Consecuencia)	Efectos que puede generar la materialización del riesgo sobre la entidad, tales como afectaciones económicas, presupuestales, operativas, legales o reputacionales.
Causa inmediata	Circunstancias o situaciones evidentes que favorecen la ocurrencia del riesgo, pero que no constituyen su origen principal.
Evento de riesgo (¿Qué puede ocurrir?)	Situación o suceso incierto que podría afectar el cumplimiento de los objetivos institucionales o de los procesos.
Causa raíz (¿Por qué puede ocurrir?)	Razón fundamental que origina el riesgo y sobre la cual deben diseñarse los controles.
Subcausas o condiciones contribuyentes	Factores que facilitan la ocurrencia del riesgo y que pueden clasificarse en humanos, tecnológicos, normativos, organizacionales o ambientales.
Redacción del riesgo	Debe ser clara, específica y concreta, describiendo qué podría suceder y evitando formulaciones genéricas.

Elemento	Punto clave
Análisis de causas	Debe diferenciar claramente la causa raíz de la causa inmediata e identificar todas las causas relevantes asociadas al riesgo.
Estructura recomendada	Evento de riesgo + causa raíz + impacto (consecuencia).

Fuente: Elaboración propia – Oficina Asesora de Planeación. Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025) del Departamento Administrativo de la Función Pública (DAFP).

Ejemplo:

Componente	Descripción
Evento de riesgo	Pérdida de información institucional.
Causa raíz	Deficiencias en los mecanismos de respaldo y recuperación de la información.
Impacto	Afectación de la continuidad de la operación y de la prestación del servicio.

Fuente: Elaboración propia – Oficina Asesora de Planeación. Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025) del Departamento Administrativo de la Función Pública (DAFP).

10.2 Análisis de riesgo inherente

Se realizará el análisis del riesgo inherente con el fin de determinar el nivel de exposición inicial de los riesgos identificados, previo a la aplicación de controles. Este análisis se efectuará mediante la valoración de la probabilidad de ocurrencia y del impacto potencial sobre el cumplimiento de los objetivos institucionales, considerando factores económicos, reputacionales, operativos, legales y demás aspectos que resulten aplicables. El resultado de esta valoración permitirá establecer el nivel de riesgo inherente y servirá como base para la evaluación de controles, la determinación del riesgo residual, la definición de tratamientos y la toma de decisiones frente a la gestión integral del riesgo.

10.2.1 Probabilidad

Se define la probabilidad, de acuerdo con la exposición del riesgo, el número de veces que se pasa por el punto de riesgo en 1 año, para lo cual el DAFP ha establecido criterios así:

Tabla 10. Criterios para definir la probabilidad

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

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

Nota: Dependiendo del tamaño y complejidad de los procesos de la entidad, los rangos de análisis de la frecuencia de la actividad de la tabla 9 podrán ser ajustados o adaptados a las necesidades, *ampliando los valores en afectación económica; en cuanto a afectación reputacional es viable mantener la estructura propuesta, o bien precisar los aspectos que se consideren pertinentes, pero siempre manteniendo los niveles y porcentajes asignados, con el fin de no afectar la estructura metodológica*

10.2.2 Impacto

La valoración del impacto de los riesgos deberá realizarse considerando las afectaciones económicas y reputacionales que puedan derivarse de su materialización, integrando en estas categorías los posibles efectos financieros, legales, operativos, presupuestales, sancionatorios y de imagen institucional, con el propósito de garantizar una valoración objetiva, homogénea y consistente en toda la Entidad. Los criterios para determinar el nivel de impacto se establecen en la Tabla 11.

Tabla 11. Criterios para definir el nivel de impacto

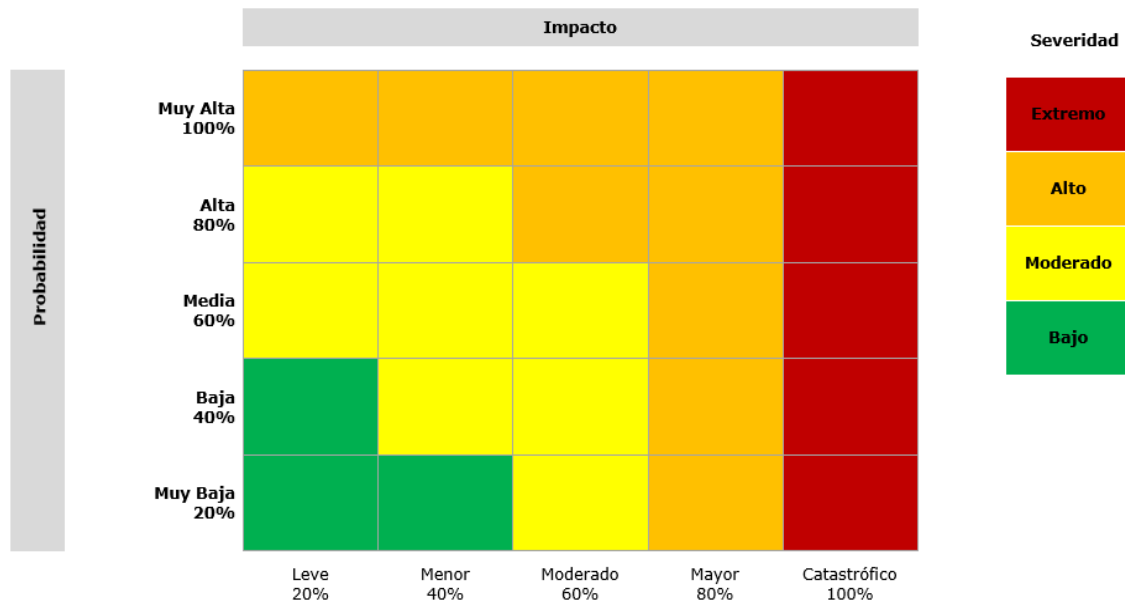
Nivel de impacto	Afectación económica	Afectación reputacional
Leve - 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
Menor - 40%	Mayor a 10 SMLMV y menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas o de proveedores.
Moderado - 60%	Mayor a 50 SMLMV y menor a 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor - 80%	Mayor a 100 SMLMV y menor a 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel del sector administrativo, nivel departamental o municipal.
Catastrófico - 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Fuente: Adaptado -Actualizada Dirección de Gestión y Desempeño Institucional de Función Pública, 2025.

Análisis de severidad

El nivel de severidad del riesgo se determinará a partir de la combinación de la probabilidad y el impacto, permitiendo establecer **el nivel de riesgo inherente** y definir las prioridades de tratamiento y monitoreo.

Figura 5. Matriz de calor para el análisis de severidad del riesgo inherente



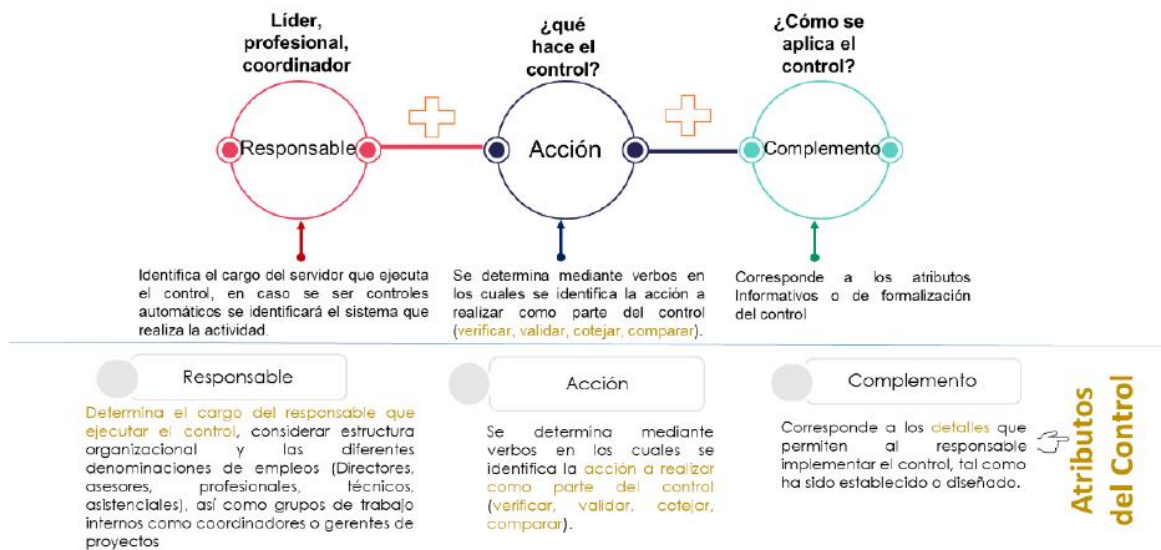
Fuente: Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025) del Departamento Administrativo de la Función Pública (DAFP).

10.3 Diseño y análisis de controles

Con base en los resultados de la valoración de factores internos y/o externos, la entidad definirá e implementará controles y acciones ante desviaciones para el tratamiento orientadas a evitar, reducir, compartir, transferir o aceptar los riesgos, según corresponda. Los riesgos que superen los niveles de tolerancia establecidos deberán contar con acciones de tratamiento y seguimiento específico.

10.3.1 Estructura para la Descripción del Control

Figura 6. Estructura redacción controles



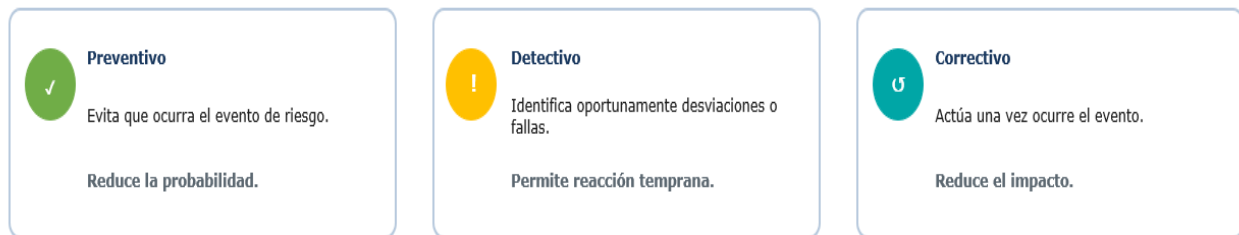
De acuerdo con lo establecido en la Guía para la Gestión Integral del Riesgo en Entidades Públicas, los componentes mínimos del control son:

Tabla 12. Componentes mínimos del control

Elemento	Descripción
Responsable	Quién ejecuta el control.
Documentación	Procedimiento, manual o instructivo que lo soporta.
Frecuencia	Periodicidad de ejecución adecuada al nivel de exposición.
Evidencia	Registro que demuestra su aplicación.
Ejecución	Forma en que se aplica y verifica.

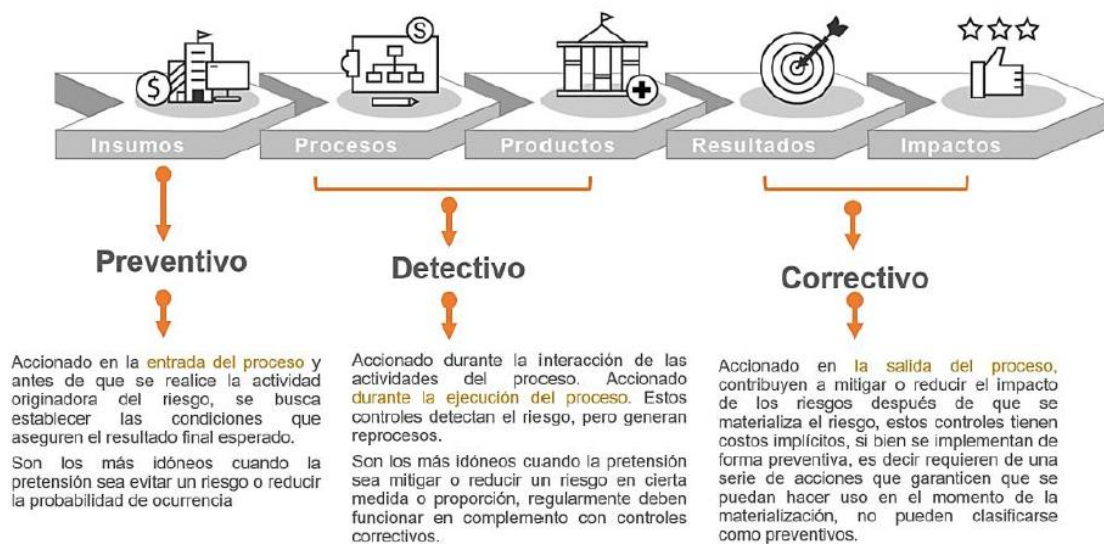
10.3.2 Tipos de control:

Para el desarrollo de las actividades de control es relevante tener en cuenta las siguientes tipologías de controles:



Con el fin de establecer en qué momento se activa el control en función de las actividades clave del proceso, base para la definición de los controles aplicables en sus 3 tipologías, se presenta a continuación la cadena de valor del proceso u las tipologías de controles:

Figura 7. Cadena de valor del proceso y las tipologías de controles



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

10.3.3 Criterios de valoración de controles

La valoración de los controles se realizará mediante la evaluación de sus características de eficiencia, con el propósito de determinar su contribución a la reducción de la probabilidad y/o el impacto de los riesgos identificados. Para tal efecto, se considerarán dos variables principales: el tipo de control y su nivel de implementación. Los controles preventivos tendrán una mayor valoración por su capacidad para evitar la ocurrencia del riesgo, seguidos de los controles detectivos y correctivos. De igual forma, los controles automáticos tendrán una valoración superior a los controles manuales, dado que reducen la intervención humana y favorecen la consistencia en su ejecución. Los criterios y ponderaciones aplicables para la valoración de los controles se establecen en la Tabla 11.

Tabla 13. Criterios de valoración de controles

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
*Implementación	Automático	25%
	Manual	15%

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

Nota*: En implementación no se tienen controles semiautomáticos.

10.4 Valoración de Riesgo Residual

La valoración del riesgo residual permite determinar el nivel de exposición al riesgo que permanece después de aplicar y valorar la efectividad de los controles implementados. Su resultado constituye un insumo para la toma de decisiones, la priorización de acciones de tratamiento y la verificación de la alineación del riesgo con los niveles de capacidad, apetito y tolerancia definidos por la Entidad.

La entidad determinará el riesgo residual mediante la aplicación de la efectividad de los controles sobre la probabilidad y el impacto del riesgo inherente, considerando que los controles actúan de manera acumulativa y pueden reducir la probabilidad de ocurrencia, el impacto o ambas variables. El resultado obtenido permitirá establecer la ubicación final del riesgo en la matriz de calor institucional

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 52 de 64
---	---	--

e identificar la necesidad de implementar acciones adicionales de tratamiento, mitigación o fortalecimiento de controles.

Los riesgos residuales deberán ser objeto de seguimiento y monitoreo periódico por parte de los responsables de proceso, con el fin de verificar la efectividad de los controles y asegurar que los niveles de exposición se mantengan dentro de los parámetros aceptados por la entidad. Cuando el riesgo residual supere los niveles de apetito o tolerancia definidos, se deberán adoptar las medidas de tratamiento correspondientes para reducir su exposición a niveles aceptables.

10.4.1 Consolidación Mapa de Riesgos Institucional:

Con base en la aplicación de la metodología de gestión integral del riesgo, la entidad consolidará el Mapa de Riesgos Institucional que permite visualizar de manera articulada las diferentes tipologías de riesgo aplicables a cada proceso. Este mapa refleja las características, complejidad operativa, interacciones, recursos, productos, servicios y grupos de valor asociados a cada proceso, con el fin de contar con una visión integral que facilite la toma de decisiones, el seguimiento y la gestión oportuna de los riesgos institucionales.

11. Gestión preventiva de riesgos fiscales

La JPMP gestionará de manera preventiva los riesgos fiscales asociados a la administración, manejo, custodia y utilización de bienes, recursos públicos e intereses patrimoniales de naturaleza pública, con el propósito de proteger el patrimonio del Estado, fortalecer la transparencia institucional y prevenir la materialización de situaciones que puedan generar daño fiscal.

El análisis de estos riesgos deberá integrarse al Mapa de Riesgos Institucional y desarrollarse bajo el esquema de líneas de defensa y los principios del Sistema de Control Interno.

Para la gestión de los riesgos fiscales, la entidad observará los siguientes lineamientos:

- Identificar los procesos, actividades y actuaciones que impliquen gestión fiscal o administración de recursos públicos.
- Reconocer los puntos de riesgo fiscal, las circunstancias inmediatas, los posibles efectos económicos y las causas raíz que puedan generar afectaciones al patrimonio público.

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 53 de 64
---	---	---

- Valorar los riesgos fiscales considerando su probabilidad de ocurrencia y el impacto económico potencial sobre bienes, recursos o intereses patrimoniales de naturaleza pública.
- Diseñar e implementar controles preventivos, detectivos o correctivos orientados a evitar, reducir o corregir las situaciones que puedan ocasionar daño fiscal.
- Realizar seguimiento periódico a la efectividad de los controles, así como a la evolución de la exposición al riesgo fiscal y a las acciones de tratamiento definidas.
- Incorporar los riesgos fiscales al proceso de monitoreo institucional para facilitar la toma de decisiones y la mejora continua de la gestión pública.

12. Riesgos de Seguridad de la Información

La JPMP gestionará los riesgos asociados a la seguridad de la información y la seguridad digital con el propósito de preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información institucional conforme a los requisitos establecido NTC ISO 27001, fortaleciendo la continuidad de la operación, la resiliencia organizacional y la protección de los activos de información que soportan el cumplimiento de la misionalidad.

Para la gestión de los riesgos de seguridad de la información, la entidad tendrá en cuenta los siguientes lineamientos:

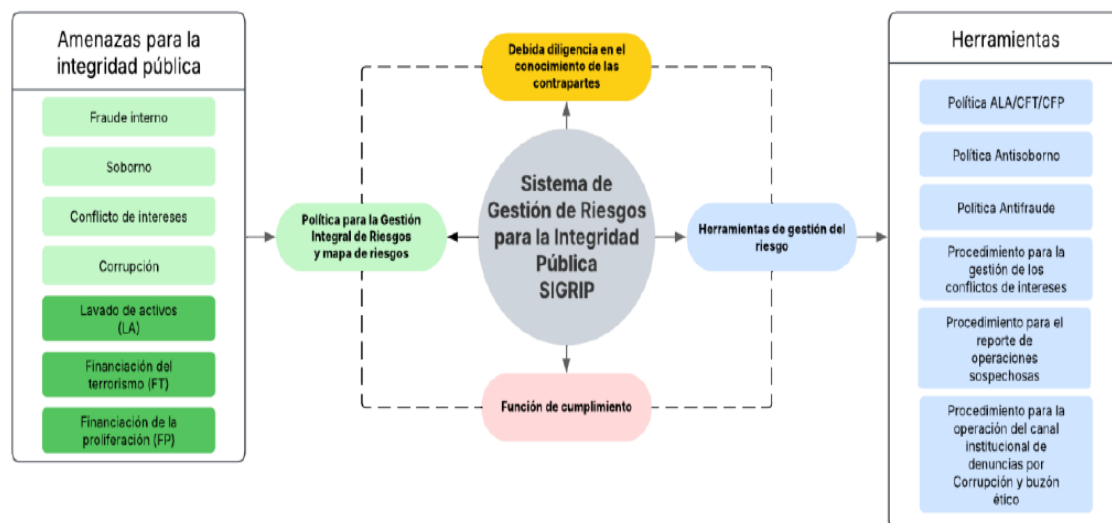
- Identificar los activos de información, servicios tecnológicos, infraestructuras y recursos que soportan los procesos institucionales.
- Reconocer las amenazas, vulnerabilidades y factores de riesgo que puedan afectar la confidencialidad, integridad o disponibilidad de la información.
- Analizar y valorar los riesgos considerando la probabilidad de ocurrencia, el impacto potencial y la criticidad de los activos de información involucrados.
- Diseñar e implementar controles preventivos, detectivos y correctivos orientados a prevenir incidentes, fortalecer la seguridad digital y reducir la exposición al riesgo.
- Realizar seguimiento permanente a la efectividad de los controles, la evolución de los riesgos y la ocurrencia de incidentes de seguridad.
- Promover la mejora continua de la gestión de riesgos de seguridad de la información mediante la actualización de controles, la gestión de incidentes, las lecciones aprendidas y el fortalecimiento de capacidades institucionales.

13. Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP

La entidad implementará el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) como mecanismo para fortalecer la integridad institucional, promover una cultura de legalidad y prevenir, detectar, controlar y monitorear los riesgos que puedan afectar el ejercicio íntegro de la función pública, la confianza ciudadana y el cumplimiento de los objetivos institucionales.

Su implementación, se desarrollará de manera articulada con el Programa de Transparencia y Ética Pública (PTEP), el Sistema de Control Interno y el Modelo de Gestión Integral del Riesgo Institucional. Para su operación, la JPMP contará con herramientas de gestión orientadas a la prevención, detección y tratamiento de los riesgos para la integridad pública, entre las que se encuentran la Política de Lucha contra la Corrupción y Antisoborno, los procedimientos para la gestión de conflictos de interés, los mecanismos de debida diligencia para el conocimiento de terceros y contrapartes, y los canales institucionales de denuncia y buzón ético. La aplicación de estas herramientas contribuirá al fortalecimiento de la cultura de integridad, la transparencia, el cumplimiento normativo y la protección de los recursos e intereses institucionales.

Figura 8. Sistema de Gestión de Riesgos para la Integridad Pública



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

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 55 de 64
---	---	--

13.1 Riesgos para la Integridad Pública

Se gestionará de manera preventiva los riesgos asociados a la integridad pública, mediante la identificación, análisis, valoración, tratamiento y monitoreo de situaciones que puedan afectar los principios de transparencia, legalidad, ética, responsabilidad y buen gobierno. Para tal efecto, la entidad incorporará en su gestión los siguientes ámbitos de riesgo:

- **Soborno:** La entidad adoptará mecanismos para prevenir, detectar y gestionar situaciones relacionadas con la oferta, entrega, solicitud o aceptación de beneficios indebidos que puedan influir en decisiones, actuaciones o procesos institucionales.
- **Fraude:** se identificará y gestionará los riesgos derivados de acciones u omisiones encaminadas a obtener beneficios indebidos mediante engaño, ocultamiento, abuso de confianza o cualquier práctica irregular que afecte los recursos públicos o el cumplimiento de los objetivos institucionales.
- **Corrupción:** La JPMP mantendrá un criterio de cero tolerancia frente a conductas que impliquen el uso indebido del poder, la función pública o los recursos institucionales para obtener beneficios particulares, garantizando la implementación de controles y acciones de prevención permanentes.
- **Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FP) :** La entidad implementará mecanismos de gestión que permitan identificar, evaluar, controlar y monitorear riesgos asociados a operaciones, relaciones, transacciones o terceros que puedan facilitar actividades relacionadas con el lavado de activos, la financiación del terrorismo o la proliferación de armas de destrucción masiva, de conformidad con la normatividad aplicable y los lineamientos institucionales adoptados.
- **Sistema de Gestión del Riesgo para la Integridad Pública:** la gestión de los riesgos para la integridad pública se desarrollará considerando el contexto institucional, la identificación y valoración de riesgos, la debida diligencia sobre terceros cuando aplique, la implementación de controles y mecanismos de tratamiento, así como el monitoreo, seguimiento y mejora continua, garantizando una actuación transparente, ética y orientada a la protección del interés público.

Nota: La identificación, análisis, evaluación, valoración, tratamiento, monitoreo y seguimiento de los **riesgos de gestión, riesgos fiscales, riesgos de seguridad**

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 56 de 64
---	---	---

de la información y riesgos para la integridad pública se desarrollarán de conformidad con los lineamientos establecidos en la **Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7**, la metodología definida en el **numeral 10 de la presente Política** y los demás instrumentos metodológicos adoptados por la Justicia Penal Militar y Policial, garantizando su aplicación bajo un enfoque integral, preventivo y articulado con el Sistema de Control Interno, el esquema de líneas de defensa y los demás mecanismos institucionales para la gestión del riesgo.

14. Tratamiento y control de los riesgos fiscales, de seguridad de la información y de integridad pública.

Los riesgos fiscales, de seguridad de la información y de integridad pública deberán gestionarse de acuerdo con los criterios institucionales de capacidad, apetito y tolerancia al riesgo, mediante la implementación de controles y acciones orientadas a prevenir, detectar o corregir situaciones que puedan generar daño al patrimonio público.

Cuando los niveles de riesgo residual superen los criterios definidos por la entidad, deberán implementarse acciones de tratamiento y fortalecimiento de controles que permitan reducir la exposición al riesgo y asegurar una adecuada gestión de los recursos público.

Nota: La identificación, análisis, evaluación, valoración, tratamiento, monitoreo y seguimiento de los **riesgos de gestión, riesgos fiscales, riesgos de seguridad de la información y riesgos para la integridad pública** se desarrollarán de conformidad con los lineamientos establecidos en la **Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7**, la metodología definida en el **numeral 10 de la presente Política** y los demás instrumentos metodológicos adoptados por la Justicia Penal Militar y Policial, garantizando su aplicación bajo un enfoque integral, preventivo y articulado con el Sistema de Control Interno, el esquema de líneas de defensa y los demás mecanismos institucionales para la gestión del riesgo.

15. Opciones de Manejo del Riesgo

Tipo de riesgo	Zona de riesgo residual	Opción de manejo	Lineamientos institucionales
Riesgos de gestión, estratégicos, operativos, de seguridad de la información, seguridad digital, ambientales, SST y demás riesgos susceptibles de aceptación	Baja	Aceptar	El riesgo podrá aceptarse cuando se encuentre dentro del apetito y la tolerancia definidos por la entidad. Se mantendrán los controles existentes y el monitoreo periódico. No será obligatorio formular un plan de tratamiento, salvo que se evidencien cambios en el contexto, debilidades en los controles, materializaciones, alertas de los KRI o instrucciones de la Línea Estratégica. La aceptación deberá quedar documentada por el líder del proceso en DARUMA.
Riesgos de gestión, estratégicos, operativos, de seguridad de la información, seguridad digital, ambientales, SST y demás riesgos susceptibles de aceptación	Moderada	Aceptar con monitoreo reforzado o reducir	El líder del proceso evaluará si el riesgo se encuentra dentro del apetito y la tolerancia institucional. Si está dentro de los límites aceptados, podrá mantenerse con controles y monitoreo reforzado. Si se aproxima al umbral de tolerancia, presenta tendencia creciente, controles débiles o consecuencias relevantes, deberán formularse acciones preventivas o un plan de tratamiento. La decisión y su justificación deberán registrarse en DARUMA.
Riesgos de gestión, estratégicos, operativos, de seguridad de la información, seguridad digital, ambientales, SST y demás riesgos susceptibles de aceptación	Alta	Reducir, evitar, transferir o compartir	El riesgo no deberá aceptarse sin medidas adicionales. El líder del proceso deberá formular e implementar un plan de tratamiento orientado a reducir la probabilidad, el impacto o ambas variables. Cuando sea jurídica, técnica y económicamente viable, podrá evitarse la actividad generadora o transferirse o compartirse parte de sus consecuencias. El plan deberá contener acciones, responsable, fecha de ejecución, recursos, entregable, indicador y meta.
Riesgos de gestión, estratégicos, operativos, de seguridad de la información, seguridad digital, ambientales, SST y demás riesgos susceptibles de aceptación	Extrema	Evitar o reducir de manera inmediata	El riesgo será considerado no aceptable. El líder del proceso deberá adoptar medidas inmediatas de contención y formular un plan de tratamiento prioritario. El evento deberá escalar a la Oficina Asesora de Planeación y a la instancia competente de la Línea Estratégica. Cuando no sea posible reducirlo oportunamente, se deberá evaluar la suspensión, modificación o eliminación de la actividad que origina la exposición, de acuerdo con las competencias y la viabilidad institucional.
Riesgos de corrupción, fraude, soborno, gestión inadecuada de conflictos de interés y LA/FT/FP	Baja	Reducir y mantener tratamiento permanente	No procede su aceptación por el solo hecho de ubicarse en zona baja. Deberán mantenerse controles preventivos y detectivos, acciones de tratamiento, debida diligencia cuando corresponda, monitoreo permanente y mecanismos de reporte. La entidad aplicará el criterio de cero tolerancia definido para estas conductas.

Tipo de riesgo	Zona de riesgo residual	Opción de manejo	Lineamientos institucionales
Riesgos de corrupción, fraude, soborno, gestión inadecuada de conflictos de interés y LA/FT/FP	Moderada	Reducir o evitar	Será obligatorio formular o fortalecer el plan de tratamiento. Se deberán revisar las causas, la segregación de funciones, la discrecionalidad, los mecanismos de debida diligencia, los canales de denuncia, la trazabilidad de las decisiones y la efectividad de los controles. El seguimiento deberá efectuarse con una frecuencia proporcional a la criticidad del riesgo.
Riesgos de corrupción, fraude, soborno, gestión inadecuada de conflictos de interés y LA/FT/FP	Alta	Reducir o evitar con intervención prioritaria	Se requerirá intervención prioritaria, fortalecimiento inmediato de controles y escalamiento a las instancias competentes. El líder del proceso deberá establecer acciones específicas para controlar las causas identificadas, reducir la discrecionalidad, fortalecer la trazabilidad y prevenir la materialización. No podrá justificarse la aceptación del riesgo residual.
Riesgos de corrupción, fraude, soborno, gestión inadecuada de conflictos de interés y LA/FT/FP	Extrema	Evitar y reducir inmediatamente	Se deberán activar medidas inmediatas de contención, revisar o suspender la actividad expuesta cuando sea procedente y escalar la situación a la Línea Estratégica y a las demás instancias competentes. El tratamiento deberá ser prioritario y permanecer activo hasta reducir la exposición. Si existen hechos materializados o señales de alerta, se aplicarán los protocolos institucionales de reporte y respuesta.
Riesgos fiscales	Baja	Reducir y mantener controles	No procede su aceptación automática. Se deberán mantener controles para proteger los bienes, recursos e intereses patrimoniales públicos y realizar monitoreo sobre el punto de riesgo fiscal. Si el riesgo residual se encuentra controlado, podrá mantenerse sin acciones adicionales, pero deberá conservar controles, responsables, evidencias y seguimiento documentado.
Riesgos fiscales	Moderada	Reducir	Será obligatorio evaluar y, cuando corresponda, fortalecer los controles asociados con la administración, custodia, adquisición, disposición, recaudo, pago o manejo de recursos públicos. Cuando los controles existentes no sean suficientes, deberá formularse un plan de tratamiento.
Riesgos fiscales	Alta	Reducir, evitar o transferir	Se deberá implementar un plan de tratamiento obligatorio y prioritario. Las acciones deberán orientarse a prevenir el daño patrimonial, fortalecer la supervisión, la segregación de funciones, la custodia, la trazabilidad y la verificación de las operaciones. La transferencia mediante pólizas u otros mecanismos no sustituye los controles preventivos.

Tipo de riesgo	Zona de riesgo residual	Opción de manejo	Lineamientos institucionales
Riesgos fiscales	Extrema	Evitar y reducir inmediatamente	Se deberán adoptar medidas inmediatas para impedir una posible afectación al patrimonio público, escalar el riesgo a las instancias competentes y revisar la continuidad o modificación de la actividad generadora. El seguimiento deberá mantenerse hasta comprobar la reducción efectiva de la exposición.

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

Notas

Nota 1. La zona de riesgo residual se determina después de valorar la efectividad de los controles sobre el riesgo inherente. La decisión de manejo deberá considerar la tipología del riesgo, el apetito, la tolerancia, el umbral, la efectividad de los controles y las obligaciones legales aplicables.

Nota 2. La ubicación de un riesgo en zona baja no implica su aceptación automática. La decisión deberá atender la tipología del riesgo y los criterios institucionales definidos en esta política.

Nota 3. Los riesgos de corrupción, fraude, soborno, gestión inadecuada de conflictos de interés, LA/FT/FP y los riesgos fiscales no podrán aceptarse únicamente por encontrarse en zona residual baja. Estos riesgos deberán mantener controles, tratamiento y monitoreo conforme al criterio institucional de cero tolerancia o protección del patrimonio público.

Nota 4. La transferencia o distribución de las consecuencias mediante pólizas, garantías, contratos u otros mecanismos legalmente permitidos no elimina la responsabilidad de implementar controles preventivos, detectivos o correctivos.

Nota 5. Los planes de tratamiento deberán registrarse en el módulo de riesgos de DARUMA e incluir, como mínimo: acción, responsable, fecha de inicio y terminación, entregable o evidencia, indicador, meta y estado de avance.

Nota 6. Una vez ejecutadas las acciones, el líder del proceso deberá evaluar su efectividad y determinar si redujeron la probabilidad, el impacto o ambos. Cuando las acciones no produzcan el resultado esperado, deberán ajustarse los controles, reformularse el tratamiento y actualizarse la valoración residual.

Nota 7. Las desviaciones significativas, la superación de los umbrales KRI, la materialización del riesgo o los cambios relevantes en el contexto obligarán a revisar la valoración, los controles y la opción de manejo, independientemente de la zona residual.

16. Acciones ante los riesgos materializados

En el evento de materializarse un riesgo identificado en el Mapa Integral de Riesgos Institucional, el responsable del proceso deberá activar de manera inmediata las acciones de respuesta definidas, implementar las medidas de contención necesarias para controlar sus efectos y realizar el análisis de las causas que dieron origen a su ocurrencia. Así mismo, se deberán evaluar las consecuencias generadas sobre los objetivos institucionales, los recursos, los bienes, la prestación del servicio, la información o la reputación institucional, según corresponda. Para ello, se aplicarán las siguientes acciones:

Tabla 14. Acciones riesgos materializados

Tipo de riesgo	Responsable	Acción
Riesgos de gestión, fiscales, corrupción e integridad pública	Líder del proceso	Notificar la materialización, activar la respuesta y adoptar acciones inmediatas de contención sobre objetivos, recursos, bienes, información o reputación institucional.
	Líder del proceso	Analizar causas, identificar fallas de control y definir acciones correctivas, preventivas o de mejora para evitar recurrencia.
	Oficina Asesora de Planeación	Acompañar metodológicamente, consolidar la información, verificar la actualización del Mapa de Riesgos y hacer seguimiento a las acciones.
	Comité Institucional de Gestión y Desempeño y/o Comité Institucional de Coordinación de Control Interno	Conocer los eventos de impacto significativo, analizar las medidas adoptadas y orientar decisiones para fortalecer la gestión del riesgo.
	Oficina de Control Interno	Evaluar de manera independiente la gestión realizada, verificar la efectividad de las acciones y formular recomendaciones de mejora.
Riesgos de seguridad de la información y seguridad digital	Responsable del activo de información y/o OTIC	Activar la gestión de incidentes, contener el evento, proteger confidencialidad, integridad y disponibilidad, y restablecer la operación cuando aplique.
	Responsable del proceso	Analizar causas del incidente, documentar consecuencias, actualizar la valoración y fortalecer controles asociados.

Tipo de riesgo	Responsable	Acción
	Oficina Asesora de Planeación	Hacer seguimiento a las acciones implementadas y verificar la actualización del mapa de riesgos, controles y planes de tratamiento.
	Oficina de Control Interno	Evaluar la respuesta institucional, verificar controles y emitir recomendaciones para prevenir eventos similares.

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

Nota: La materialización de un riesgo deberá generar revisión de la valoración, evaluación de controles, documentación de lecciones aprendidas y definición de acciones de mejora para fortalecer el Sistema de Control Interno, actualizar el Mapa Integral de Riesgos Institucional y prevenir recurrencia, esta debe ser registrada en el módulo de riesgos del aplicativo DARUMA.

17. Monitoreo, seguimiento auditoría y supervisión al mapa de riesgos institucional y controles.

Con el fin de verificar la efectividad de los controles, asegurar la ejecución de los planes de tratamiento y fortalecer la mejora continua de la gestión del riesgo, la JPMP establecerá mecanismos de monitoreo, seguimiento, evaluación independiente y supervisión, de conformidad con el esquema de líneas de defensa y las responsabilidades definidas para cada actor institucional, las cuales se presentan a continuación:

Tabla 14. Roles, responsabilidades y frecuencia para el monitoreo y seguimiento del mapa de riesgos institucional y controles.

Reporte	Responsable	Descripción	Frecuencia
Monitoreo	Líder de la dependencia o proceso	Realizará el registro de evidencias, validación y monitoreo de los riesgos, controles y planes de tratamiento (en los casos que aplique), por medio del aplicativo DARUMA – Módulo de Riesgos.	Cuatrimestral

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 62 de 64
---	---	--

Reporte	Responsable	Descripción	Frecuencia
Seguimiento (administración)	Oficina Asesora de Planeación	Realizará el seguimiento de los controles de acuerdo con la frecuencia establecida, por medio del aplicativo DARUMA, en el cual se registrará los avances alcanzados en el periodo.	Cuatrimestral
Auditoría	Oficina de Control Interno de Gestión	Realizará la evaluación de los controles y riesgos, por medio del aplicativo DARUMA, de acuerdo con la frecuencia establecida, generando informe para cada periodo de los resultados obtenidos.	Semestral
Supervisión	Comité Institucional de Gestión y Desempeño	Se presentará los informes del proceso de Monitoreo, Seguimiento y Auditoria, con el fin de socializar resultados de la gestión por periodo y establecer posibles acciones de mejora.	Semestral

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

17.1 Mejora continua

La **Justicia Penal Militar y Policial (JPMP)** promoverá la mejora continua de la Gestión Integral del Riesgo mediante la revisión periódica de los riesgos, la evaluación de la efectividad de los controles, el seguimiento a los planes de tratamiento, el análisis de riesgos materializados y la implementación de acciones de mejora.

Este proceso se desarrollará de manera articulada con el **Modelo Integrado de Planeación y Gestión (MIPG)**, el **Sistema de Control Interno**, el **Programa de Transparencia y Ética Pública (PTEP)**, el **Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP)** y los demás instrumentos institucionales aplicables, con el fin de fortalecer la prevención, la toma de decisiones y el cumplimiento de los objetivos institucionales.

Para apoyar la administración, seguimiento, monitoreo y control de la Gestión Integral del Riesgo, la JPMP utilizará el aplicativo **DARUMA** o la herramienta tecnológica que haga sus veces. A través de esta herramienta se gestionará la información relacionada con los riesgos institucionales, los controles, las acciones

	JUSTICIA PENAL MILITAR Y POLICIAL Política para la Gestión Integral de Riesgos Institucionales	Página 63 de 64
---	---	--

de tratamiento, los riesgos materializados, los planes de mejoramiento y demás elementos definidos en la metodología institucional de gestión del riesgo, facilitando el seguimiento, la trazabilidad y la mejora continua del sistema.

18. Anexos.

- **Decreto 1122 de 2024 y anexo técnico**
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=250176>
- **Mapa de Riesgos Institucional**, como instrumento oficial para la identificación, valoración, tratamiento y seguimiento de los riesgos institucionales. <https://www.justiciamilitar.gov.co/participa/programa-de-transparencia-y-etica-publica-plan-anticorrupcion-y-de-atencion-al-ciudadano>
- **Programa de Transparencia y Ética Pública (PTEP)**, como instrumento de gestión para la prevención de la corrupción, el fortalecimiento de la integridad pública y la transparencia institucional. <https://www.justiciamilitar.gov.co/participa/programa-de-transparencia-y-etica-publica-plan-anticorrupcion-y-de-atencion-al-ciudadano>
- **Anexo Técnico del Programa de Transparencia y Ética Pública**, que desarrolla los componentes metodológicos y mecanismos de seguimiento definidos por la Entidad. <https://www.justiciamilitar.gov.co/participa/programa-de-transparencia-y-etica-publica-plan-anticorrupcion-y-de-atencion-al-ciudadano>
- **Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025)**, expedida por el Departamento Administrativo de la Función Pública (DAFP), como referente metodológico para la gestión integral del riesgo en la JPMP. https://www.funcionpublica.gov.co/documents/d/quest/2025-09-11_guia_gestion_integral_riesgo_v7?download=true

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá D.C.,

CONTROL DE CAMBIOS			
Versión	Fecha	Instancia de Aprobación	Descripción
01	08/07/2024	Comité Institucional de Coordinación de Control Interno (CICCI). Sesión 1.	Elaboración inicial del documento.
02	08/07/2025	Comité Institucional de Coordinación de Control Interno (CICCI). Sesión 1.	Se realizó ajuste de acuerdo con la "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, V6" , así como lo consignado en el anexo técnico del Decreto 1122 de 2024, con relación a los roles de las líneas de defensa.
03	24/09/2026	Comité Institucional de Coordinación de Control Interno (CICCI). Sesión 3.	Actualización integral de la Política de Gestión Integral del Riesgo conforme a la Guía DAFP V.7 (2025), incorporando Gobierno del Riesgo, gestión de oportunidades, capacidad, apetito y tolerancia al riesgo, riesgos emergentes, fortalecimiento de líneas de defensa, integración del PTEP y SIGRIP, gestión de riesgos fiscales, integridad pública, seguridad de la información y seguridad digital, así como la actualización del marco metodológico y de seguimiento de la gestión del riesgo.