

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

TABLA DE CONTENIDO

INTRODUCCIÓN	2
DEFINICIONES	2
1. DECLARACIÓN DE VALOR DE LA POLÍTICA	4
2. NORMATIVIDAD	5
3. OBJETIVOS	6
3.1. Objetivo General	6
3.2. Objetivos Específicos	6
4. ALCANCE	7
5. LINEAMIENTOS GENERALES	7
5.1. Contexto Estratégico de la UPME	7
5.1.1. Factores Externos	8
5.1.2. Factores Internos	9
5.2. Apetito y Tolerancia al Riesgo / Niveles de Aceptación	10
5.3. Esquema de Gestión Integral del Riesgo	11
5.3.1. Descripción General de la Metodología	11
5.3.3. Acciones Ante la Materialización de Riesgos (Gestión de Eventos) ¹⁴	
5.3.4. Información, Comunicación y Reporte	15
5.3.5. Niveles de Responsabilidad y Autoridad Frente a la Administración del Riesgo en la Entidad (acorde con el esquema de líneas de defensa)	16
6. ACTUALIZACIÓN	20
7. COMUNICACIÓN Y DIVULGACIÓN	21
8. ANEXOS	21
9. DOCUMENTOS RELACIONADOS	21
10. CONTROL DE CAMBIOS	21

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

INTRODUCCIÓN

El presente documento establece la Política para la Gestión Integral de Riesgos de la Unidad de Planeación Minero-Energética, en adelante UPME, la cual contiene los lineamientos para la revisión del contexto, la identificación, valoración, tratamiento, monitoreo y seguimiento, comunicación y consulta de los riesgos que puedan afectar el cumplimiento de la misión, los objetivos estratégicos, la gestión de los procesos y la integridad pública (SIGRIP), lo cual abarca riesgos generales de la gestión, gestión preventiva de riesgos fiscales, riesgos de seguridad de la información y las amenazas para la integridad pública relacionadas con soborno, fraude, inadecuada gestión del conflicto de intereses, corrupción y el Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP.

Lo anterior de acuerdo con las directrices del Modelo Integrado de Planeación y Gestión-MIPG, la responsabilidad de la línea estratégica y las líneas de defensa definidas en la Dimensión de Seguimiento, evaluación y control integral. Así mismo, se fundamenta en la "Guía para la Gestión Integral del Riesgo en Entidades Públicas" en su última versión, expedida por el Departamento Administrativo de la Función Pública – DAFP; las Normas ISO 9001, 31000 27001, el estándar internacional COSO – ERM (2017) y demás normatividad aplicable.

DEFINICIONES

Apetito de riesgo: Es el nivel de riesgo que la UPME está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección.

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida que permite reducir o mitigar un riesgo.

Corrupción: Todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral. (A partir del artículo 2.1.4.3.1.3 del Decreto 1081 de 2015)

Financiación del Terrorismo (FT): el artículo 345 de la Ley 599 de 2000, define el delito de lavado de activos como la conducta desplegada por quien "directa o indirectamente provea, recolecte, entregue, reciba, administre, aporte, custodie o guarde fondos, bienes o recursos, o realice cualquier otro acto que promueva, organice, apoye, mantenga, financie o sostenga económicamente a grupos de delincuencia organizada, grupos armados

Página 2 de 22

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

al margen de la ley o a sus integrantes, o a grupos terroristas nacionales o extranjeros, o a terroristas nacionales o extranjeros, o a actividades terroristas”. La Financiación del Terrorismo puede darse por: recaudación, transmisión, utilización.

Financiación de la Proliferación de Armas de Destrucción Masiva (FP): fondos u otros activos a disposición, directa o indirectamente, de o para el beneficio de, alguna persona o entidad designada por o bajo la autoridad del Consejo de Seguridad de las Naciones Unidas dentro del Capítulo VII de la Carta de las Naciones Unidas, en lo relativo a la prevención, represión e interrupción de la proliferación de armas de destrucción masiva y su financiamiento. La Financiación de la Proliferación puede darse por: recaudación, transmisión, utilización.

Función de cumplimiento: función que debe distribuirse dentro de la organización que asigna a una persona, grupo o dependencia la responsabilidad de adoptar medidas para promover el cumplimiento interno, administrar los riesgos para la integridad pública de conformidad con las políticas institucionales de gestión de riesgos, apoyar los procesos de evaluación de los Sistemas de Gestión del Riesgo, realizar un control de segunda línea y asesorar a la Alta Dirección en el direccionamiento estratégico de la organización desde un enfoque basado en riesgos para proteger la integridad pública.

KRI (Indicadores Clave de Riesgo): Métricas utilizadas para proporcionar una señal temprana de exposiciones al riesgo, permitiendo identificar riesgos emergentes y gestionar el desempeño.

Lavado de activos: el artículo 323 de la Ley 599 de 2000, define el delito de lavado de activos como la conducta desplegada por quien “adquiera, resguarde, invierta, transporte, transforme, almacene, conserve, custodie o administre bienes que tengan su origen mediato o inmediato en actividades [relacionadas con un delito fuente], o vinculados con el producto de delitos ejecutados bajo concierto para delinquir, o les dé a los bienes provenientes de dichas actividades apariencia de legalidad o los legalice, oculte o encubra la verdadera naturaleza, origen, ubicación, destino, movimiento o derecho sobre tales bienes o realice cualquier otro acto para ocultar o encubrir su origen ilícito”. El Lavado de Activos puede darse por: colocación, ocultamiento e integración.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Punto de Riesgo: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.

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

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información

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

Riesgos para la integridad: Toda actuación o decisión de las y los servidores públicos, así como de otros colaboradores de las entidades públicas que privilegien el interés particular sobre el general, asociadas a conductas no deseadas que van en contravía de los valores del servicio público. Incluido, también, el riesgo de que la integridad de la entidad sea utilizada para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas

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

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

Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP: esquema que define la interrelación e interacción de diferentes elementos para asegurar una gestión integral de los riesgos que afectan la integridad pública. El SIGRIP se articula con la Política para la Gestión Integral de Riesgos.

1. DECLARACIÓN DE VALOR DE LA POLÍTICA

La Unidad de Planeación Minero Energética – UPME reconoce la gestión integral de riesgos como un pilar fundamental para el cumplimiento de su misión institucional y la generación de valor público. Por ello, la Alta Dirección y, junto su equipo humano, asume el compromiso de fortalecer una cultura organizacional basada en la prevención, la transparencia, la responsabilidad y la mejora continua, que permita anticipar y gestionar oportunamente los eventos que puedan afectar el logro de los objetivos estratégicos.

A través de la identificación, valoración, tratamiento, monitoreo y seguimiento de los riesgos —incluyendo la prevención y cero tolerancia frente a riesgos de corrupción, fraude, soborno, lavado de activos y financiación del terrorismo (LA/FT/FP)—, la UPME promueve la toma de decisiones informadas, la protección de los recursos públicos, el fortalecimiento de la confianza de sus grupos de valor y el mejoramiento permanente de su desempeño institucional. Esta gestión contribuye a garantizar servicios de calidad, una administración eficiente y transparente, y el cumplimiento efectivo de su propósito de orientar la planeación integral del sector minero-energético en beneficio de la sociedad.

La gestión integral de riesgos es, así, una herramienta para transformar desafíos en oportunidades, fortalecer la capacidad institucional y asegurar la sostenibilidad de los resultados, generando valor para el país mediante una actuación ética, eficiente, innovadora y orientada al servicio y fundamentada en una sólida cultura de la legalidad y el estricto cumplimiento del Código de Integridad en el Servicio Público.

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

2. NORMATIVIDAD

- **Constitución Política de Colombia en los artículos 267 y 268.** modificados por el Acto Legislativo 04 de 2019, base del control fiscal preventivo y concomitante.
- **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. En particular, el artículo 2º, literal a), establece como objetivo del Sistema de Control Interno proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten.
- **Ley 610 de 2000.** Por la cual se establece el trámite de los procesos de responsabilidad fiscal, fundamental para la definición del daño patrimonial y riesgos fiscales.
- **Ley 599 de 2000 (Código Penal).** En lo referente a la tipificación de conductas de corrupción, Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FP).
- **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 (Estatuto Anticorrupción).
- **Ley 1712 de 2014.** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Ley 1952 de 2019 (Código General Disciplinario), modificada por la Ley 2094 de 2021.** Aplicable para la identificación y prevención de la inadecuada gestión de los conflictos de intereses.
- **Ley 2195 de 2022:** Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción, y se establece la obligatoriedad de articular la gestión de riesgos de LA/FT/FP y corrupción.
- **Decreto 1081 de 2015.** Decreto Único Reglamentario del Sector Presidencia de la República. Establece lineamientos relacionados con la transparencia, el acceso a la información pública y las estrategias para la gestión de riesgos de corrupción.
- **Decreto 1083 de 2015.** Decreto Único Reglamentario del Sector de Función Pública. En su artículo 2.2.21.5.4 establece que la administración de riesgos hace parte integral del Sistema de Control Interno y es responsabilidad de todas las entidades públicas.
- **Decreto 1499 de 2017.** Modificó el Decreto 1083 de 2015 y actualizó el Modelo Integrado de Planeación y Gestión (MIPG), articulando el Sistema de Gestión con el Sistema de Control Interno bajo el Modelo Estándar de Control Interno (MECI).
- **Decreto 1122 de 2024.** Por el cual se reglamenta la implementación de los Programas de Transparencia y Ética Pública (PTEP).
- **NTC-ISO 31000:2018.** Gestión del Riesgo. Principios y directrices. Establece las mejores prácticas internacionales para la gestión integral de riesgos aplicables a cualquier tipo de organización.
- **Documento CONPES 3854 de 2016.** Política Nacional de Seguridad Digital, que establece lineamientos para fortalecer la gestión de riesgos de seguridad digital en las entidades públicas y privadas del país.
- **Modelo Nacional de Gestión del Riesgo de Seguridad de la Información en Entidades Públicas – Anexo 4.** Departamento Administrativo de la Función Pública (DAFP), agosto de 2019. Define lineamientos para la identificación, valoración y tratamiento de riesgos de seguridad de la información en entidades públicas.

Página 5 de 22

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

- **Anexo técnico decreto 1122 de 2024.** A través del cual se definen las acciones estratégicas, los instrumentos y responsables de los componentes transversal y programático del Programa de Transparencia y Ética Pública (PTEP) en materia de riesgos para la integridad pública.
- **Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7.** Departamento Administrativo de la Función Pública (DAFP), actualizada en agosto de 2025. Establece los lineamientos metodológicos para la gestión integral de riesgos, incluidos los riesgos de gestión, corrupción, seguridad digital y continuidad institucional.
- **Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG).** Departamento Administrativo de la Función Pública (DAFP), actualizado en febrero de 2026. Define los lineamientos para la implementación y fortalecimiento del MIPG, incluyendo la Dimensión de Seguimiento, evaluación y control integral y la administración del riesgo.

3. OBJETIVOS

3.1. Objetivo General

Establecer los lineamientos, criterios y responsabilidades para la implementación y fortalecimiento del Sistema Integrado de Gestión de Riesgos Institucionales y de Integridad Pública (SIGRIP) en la UPME, mediante la identificación, análisis, valoración, tratamiento, monitoreo, seguimiento y comunicación de los riesgos y oportunidades que puedan afectar el cumplimiento de la misión institucional, los compromisos de gobierno, los objetivos estratégicos, tácticos y operativos, así como la observancia de los principios de integridad y buen gobierno.

Lo anterior, con el propósito de fortalecer la toma de decisiones basada en riesgos, promover una cultura preventiva y de autocontrol, implementar controles y acciones de tratamiento eficaces, incrementar la capacidad institucional para gestionar la incertidumbre y contribuir a la creación, protección y sostenibilidad del valor público, en articulación con el Modelo Integrado de Planeación y Gestión (MIPG), el Sistema de Control Interno y las mejores prácticas internacionales basadas en el marco COSO-ERM.

3.2. Objetivos Específicos

- Implementar un marco normativo y metodológico para la gestión integral de riesgos en la UPME, que incluya directrices claras y herramientas adecuadas para la identificación, evaluación y priorización de los riesgos institucionales, asociados con riesgos generales de la gestión, gestión preventiva de riesgos fiscales, riesgos de seguridad de la información y las amenazas para la integridad pública relacionadas con soborno, fraude, inadecuada gestión del conflicto de intereses, corrupción y el Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP, que puedan afectar el cumplimiento de los objetivos estratégicos y operacionales de la entidad, definiendo claramente los roles y responsabilidades para su administración, alineados bajo el esquema de las líneas de defensa.

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

- Diseñar e implementar un conjunto de controles para prevenir y mitigar los riesgos identificados, con un enfoque de mejora continua, garantizando la protección de los recursos públicos y el fortalecimiento de la cultura de control interno en la institución.
- Fortalecer la articulación e implementación de los instrumentos que conforman el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), garantizando la aplicación del principio de debida diligencia en el conocimiento de las contrapartes, la adecuada operación del canal institucional de denuncias y el ejercicio efectivo de la función de cumplimiento, con el fin de prevenir, detectar y gestionar oportunamente riesgos asociados a la corrupción, el fraude, el lavado de activos, la financiación del terrorismo, la financiación de la proliferación de armas de destrucción masiva (LA/FT/FP) y demás conductas que puedan afectar la integridad, la transparencia y el cumplimiento de los objetivos institucionales.
- Promover una cultura organizacional de la legalidad, transparencia y gestión integral del riesgo en la UPME, a través de la capacitación continua del personal y la sensibilización sobre la importancia del control interno, con el fin de fortalecer la capacidad institucional para cumplir con los compromisos de gobierno y los fines estratégicos de la entidad.
- Implementar y fortalecer mecanismos de monitoreo y seguimiento mediante Indicadores Clave de Riesgo (KRI), que permitan medir la exposición institucional a los riesgos, identificar tendencias y desviaciones, generar alertas tempranas para la toma oportuna de decisiones y contribuir a la efectividad de los controles, la prevención de eventos de riesgo y el cumplimiento de los objetivos estratégicos de la Entidad.

4. ALCANCE

La Política de Gestión Integral de Riesgos aplica a todos los procesos, proyectos, planes y actividades de la UPME, así como a los servidores públicos, contratistas y demás colaboradores que participen en el cumplimiento de los objetivos institucionales. Su alcance se extiende a las actividades ejecutadas mediante terceros, convenios, alianzas u otros mecanismos de articulación institucional.

En concordancia con el SIGRIP, la política contempla los riesgos asociados a los grupos de valor, contrapartes, entidades con las que la UPME interactúa, trámites, operaciones y territorios donde ejerce sus funciones. Asimismo, comprende la identificación, análisis, valoración, tratamiento, monitoreo, seguimiento, comunicación y consulta de los riesgos que puedan afectar el logro de los objetivos institucionales.

5. LINEAMIENTOS GENERALES

5.1. Contexto Estratégico de la UPME

La gestión integral de riesgos en la UPME partirá del análisis del contexto interno y externo de la entidad, con el fin de identificar los factores, los cuales se relacionan en la **iError! No se encuentra el origen de la referencia.** y **iError! No se encuentra el origen de**

Página 7 de 22

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

la referencia. , condiciones y tendencias que puedan afectar el cumplimiento de su misión, objetivos estratégicos, procesos, proyectos y la generación de valor público.

Este análisis deberá sustentarse en información institucional formalizada, datos verificables y fuentes confiables, considerando, entre otros aspectos, del contexto interno: la estructura organizacional, el direccionamiento estratégico, la capacidad institucional, los recursos disponibles, la cultura organizacional, el desempeño de los procesos, los resultados de seguimiento y evaluación, así como los cambios normativos, económicos, sociales, tecnológicos, ambientales, sectoriales y de relacionamiento con las partes interesadas.

Como parte del análisis del contexto interno y externo, la UPME considerará la estructura organizacional, los niveles de autoridad y la delegación de funciones con capacidad de decisión, especialmente en aquellos procesos que involucren la administración de recursos, la contratación, la supervisión, la regulación y demás actuaciones que puedan generar exposición a riesgos. Asimismo, se tendrán en cuenta las características de las contrapartes con las que la Entidad interactúa, los grupos de valor, aliados estratégicos, operadores, contratistas y demás terceros, así como las condiciones particulares de los territorios, jurisdicciones y ámbitos geográficos donde desarrolla sus funciones o tiene incidencia, con el fin de identificar factores que puedan influir en la materialización de riesgos y definir medidas de tratamiento acordes con el contexto institucional

La identificación y valoración de los riesgos y oportunidades deberá considerar la interacción de estos factores internos y externos, de manera que permita comprender las causas, impactos y condiciones que pueden influir en el logro de los objetivos institucionales, facilitando la definición de controles, acciones de tratamiento y estrategias de respuesta acordes con el contexto de la entidad.

5.1.1. Factores Externos

Hacen parte el entorno político, económico, social, ambiental y tecnológico; actores del sector, reguladores, organismos de control, ciudadanos y partes interesadas, así como riesgos asociados a cambios normativos y eventos externos. Sector donde opera la entidad y su relacionamiento con otras entidades e instancias necesarias para su gestión, así como entorno de desarrollo territorial:

Tabla 1 Factores Externos de Riesgo y sus Aspectos Relevantes a Considerar

FACTORES DE RIESGO	ASPECTOS RELEVANTES
Político	Cambio de gobierno y administración, nuevos directivos en la UPME, políticas asociadas al sector minero energético, la preservación del medio ambiente, la Transformación Digital e Inteligencia Artificial; los Objetivos de Desarrollo Sostenible, los objetivos y compromisos del Plan Nacional de Desarrollo, las relaciones internacionales, presiones políticas y gremiales.
Económico	Presiones inflacionarias, comportamiento de la tasa de cambio representativa del mercado (TRM), la deuda del Fondo de Estabilización de Precios de Combustibles (FEPC), PIB nacional, inversión extranjera, comportamiento de las exportaciones y de la tasa de crecimiento económico, recursos de inversión y operación, presupuesto, lineamientos para la austeridad del gasto, los compromisos de gobierno.

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

FACTORES DE RIESGO	ASPECTOS RELEVANTES
Social	Grupos étnicos, derechos humanos, organizaciones de mujeres, representantes de Asojuntas, organizaciones de campesinos, grupos ambientales, la participación ciudadana, el conflicto armado, conflicto de intereses, Objetivos de Desarrollo Sostenible, cualificación del personal, epidemias o pandemias.
Tecnológico	Nuevas tecnologías, mayor descentralización y digitalización, interoperabilidad de los sistemas de información de gobierno, plataformas tecnológicas, requisitos de MinTic, seguridad de la información, servidores internos de la Entidad (Intranet, SGI, Página Web), ecosistema digital, conocimiento y competencia del personal clave que debe gestionar esos servicios, machine learning (análisis de datos masivos y determinación de patrones), la adopción de robots de software, Big Data, Tecnologías de la 4 revolución industrial.
Ambiental	Protección ambiental, emisiones de CO2, huella de carbono, lluvia ácida, etc.; deterioro ambiental, incremento de temperatura, inundaciones, descongelamiento de los cascos polares, eventos climáticos extremos; gestión de los recursos naturales renovables, desarrollo sostenible, cambio climático, biodiversidad nacional, fenómeno del niño, fenómeno de la niña, Objetivos de Desarrollo Sostenible, epidemias o pandemias.
Legal	Ley Orgánica del Plan de Desarrollo, Código de Minas, regulación de la integración de las energías renovables no convencionales al Sistema Energético Nacional, directrices para la gestión del cambio climático, disposiciones para la transición energética, la dinamización del mercado energético y la reactivación económica del país; el Decreto Único Reglamentario del Sector Administrativo de Minas y Energía, ley por medio de la cual se promueve el abastecimiento, continuidad, confiabilidad y cobertura del gas combustible en el país; Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, ley por la cual se establecen los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG, directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado, los lineamientos generales de la política de Gobierno Digital, resolución por la cual se define e implementa un mecanismo que promueva la contratación de largo plazo para proyectos de generación de energía eléctrica complementario a los mecanismos existentes en el Mercado de Energía Mayorista, resolución por la cual se establecen los procedimientos que se deben seguir para la expansión de los Sistemas de Transmisión Regional mediante Procesos de Selección.

Fuente: Elaboración OAP

5.1.2. Factores Internos

Hacen parte la estructura organizacional, cultura institucional, capacidad tecnológica, talento humano, procesos internos, recursos financieros, políticas internas y marco normativo aplicable.

Tabla 2 Factores Internos de Riesgo y sus Aspectos Relevantes a Considerar

FACTORES DE RIESGO	ASPECTOS RELEVANTES
Talento Humano	Planta de personal, competencias del personal a partir de la implementación del Modelo Integrado de Planeación y Gestión MIPG, desarrollo de habilidades, motivación e involucramiento del personal, concurso de méritos para proveer los cargos en provisionalidad, rotación del personal, clima laboral, bienestar social, teletrabajo.
Procesos	Desactualización de la documentación, gestión por procesos, interacción entre procesos, mecanismos de gestión, autocontrol y autoevaluación; apropiación del Modelo Integrado de Planeación y Gestión MIPG, participación del personal en campañas de socialización; toma de decisiones.

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

FACTORES DE RIESGO	ASPECTOS RELEVANTES
Financieros	Recursos, necesidades por parte de las dependencias, plan anual de adquisiciones, comunicación de cambios, apropiación de recursos, comunicación entre las dependencias intervinientes en el proceso presupuestal, definición de proyectos, disponibilidad presupuestal.
Tecnología	Necesidades tecnológicas, conocimiento y aplicabilidad de las herramientas informáticas, conectividad, herramientas y aplicativos internos, teletrabajo y computación en la nube, cultura digital, manejo de archivos físicos, copias de seguridad, infraestructura tecnológica.
Estratégicos	Planificación institucional, lineamientos, mapa de procesos, estructura organizacional, políticas de operación, comunicaciones, información institucional.
Comunicación Interna	Canales internos de comunicación, manejo de la información, calidad de la información, herramientas de comunicación, cultura empresarial, plan de comunicaciones.

Fuente: Elaboración OAP

5.2. **Apetito y Tolerancia al Riesgo / Niveles de Aceptación**

En función de los riesgos residuales aprobados por los Líderes de los Procesos y registrados en los mapas oficiales de riesgos de la entidad, la UPME establece su apetito y tolerancia del riesgo de la siguiente manera:

- **Riesgos Generales de gestión, seguridad de la información, sistemas de gestión de seguridad y salud en el trabajo, y gestión ambiental:** Los riesgos residuales ubicados en las zonas Extrema y Alta de la matriz de calor se consideran por fuera del apetito de riesgo institucional; por lo tanto, deberán contar con acciones de tratamiento complementarias orientadas a reducir su probabilidad de ocurrencia y/o su impacto, hasta alcanzar niveles aceptables para la Entidad.

Los riesgos ubicados en la zona Moderada se consideran dentro del nivel de tolerancia al riesgo definido por la Entidad. En consecuencia, podrán ser aceptados siempre que se evidencie la adecuada ejecución y efectividad de los controles establecidos y se mantenga un monitoreo periódico que permita identificar oportunamente cambios en su nivel de exposición.

Por su parte, los riesgos ubicados en la zona Baja se consideran dentro del apetito de riesgo institucional y podrán ser tolerados una vez se valide, mediante los mecanismos de monitoreo y seguimiento definidos, la correcta implementación y efectividad de los controles. En todos los casos, independientemente de su nivel de riesgo residual, deberá mantenerse el monitoreo y seguimiento conforme a la periodicidad establecida por la Entidad, con el fin de verificar que las condiciones del riesgo permanezcan bajo control.

- **Riesgos para la Integridad Pública:** Los cuales contemplan soborno, fraude, inadecuada gestión del conflicto de intereses, corrupción, Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP. Para esta tipología de riesgos la UPME mantiene

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

su compromiso de cero tolerancia, en consecuencia, se deben entablar acciones de fortalecimiento para apoyar su mitigación y tratamiento.

5.3. Esquema de Gestión Integral del Riesgo

En el siguiente numeral se describen lineamientos y consideraciones necesarias para una adecuada administración del riesgo; así como los niveles de responsabilidad y autoridad acorde con el esquema de las líneas defensa:

5.3.1. Descripción General de la Metodología

Para la administración de los riesgos, la UPME toma como base las orientaciones metodológicas establecidas en la "Guía para la Gestión Integral del Riesgo en Entidades Públicas" del Departamento Administrativo de la Función Pública – DAFP en su última versión, así como las dispuestas por la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, además de la "Dimensión de Seguimiento, evaluación y control integral" del MIPG. Esto último, articulado con las políticas del MIPG correspondientes a: Planeación Institucional, Política de Evaluación y Seguimiento y la Política de Control interno, en cumplimiento del Decreto 1499 de 2017; y como referentes las normas ISO 9001, 31000 y 27001.

En línea con lo anterior, la UPME acoge los lineamientos acorde con la dinámica y necesidades de la entidad, estableciendo un esquema metodológico transversal y estandarizado para la administración de todas las tipologías de riesgo (generales, fiscales, de integridad pública y de seguridad de la información), el cual se desarrollará a través del desarrollo de cuatro (4) fases metodológicas:

5.3.1.1. Desarrollo de las Fases Metodológicas

Fase 1: Identificación y Descripción del Riesgo

En esta etapa se debe considerar la comprensión del contexto institucional, la caracterización de los procesos, la identificación de los puntos de riesgo, de las áreas de impacto y áreas de factores de riesgo.

Fase 2: Análisis del Riesgo Inherente

En esta fase se busca establecer el nivel de severidad del riesgo, mediante la determinación de la probabilidad de su ocurrencia y sus consecuencias o impacto. Los niveles para calificar la probabilidad y el impacto corresponden a los que establezca la "Guía para la Gestión Integral del Riesgo en Entidades Públicas " vigente, emitida por el DAFP y estarán contenidos de igual forma en el procedimiento de "PRO-PES-003 Gestión Integral del Riesgo".

En esta fase se debe identificar el tratamiento de los riesgos, acorde a los establecido en la Guía para la Gestión Integral del Riesgo en Entidades Públicas vigente, emitida por el DAFP (Evitar, Mitigar, Reducir, Compartir, Transferir y/ o Aceptar el Riesgo.)

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

Fase 3: Diseño y Análisis de Controles

Una vez se cuente con el nivel de severidad del riesgo inherente, se debe proceder con el establecimiento de los controles para reducirlo o mitigarlo; la descripción y valoración de los controles se realizará de acuerdo con lo establecido en la Guía para la Gestión Integral del Riesgo en Entidades Públicas vigente, emitida por el DAFP y de igual forma en el procedimiento de "PRO-PES-003 Gestión Integral del Riesgo".

Fase 4: Valoración del Riesgo Residual

El nivel de riesgo residual es el resultado de aplicar la efectividad de los controles al riesgo inherente. Esta mitigación se realiza de forma acumulativa (el impacto de un control se calcula sobre el valor resultante del control anterior).

Una vez establecido el nivel de severidad del riesgo residual, se determinará la estrategia para combatirlo de acuerdo con las opciones que relaciona la Guía para la Gestión Integral del Riesgo en Entidades Públicas vigente, emitida por el DAFP: Reducir, Compartir, Aceptar o Evitar, y los umbrales de apetito y tolerancia al riesgo del riesgo dispuestos por la UPME.

5.3.2. Monitoreo, Seguimiento y Revisión

Los monitoreos y seguimientos de la gestión de los riesgos se realizan cuatrimestralmente a través de las evidencias reportadas en la aplicación de los controles, teniendo en cuenta el esquema de las líneas de defensa descrito en el "Modelo Estándar de Control Interno – MECI – Dimensión de Seguimiento, evaluación y control integral" del MIPG y el procedimiento "PRO-PES-003 Gestión Integral del Riesgo". Para el caso de los riesgos materializados, se deberá hacer el análisis correspondiente para determinar la periodicidad del seguimiento.

Asimismo, el monitoreo de los riesgos se efectuará mediante la definición, medición y análisis de Indicadores Clave de Riesgo (Key Risk Indicators – KRI), los cuales permitirán identificar oportunamente cambios en las condiciones de riesgo y generar alertas tempranas frente a posibles eventos que puedan afectar el logro de los objetivos institucionales. Estos indicadores deberán articularse con los Indicadores Clave de Desempeño o de Proceso (Key Performance Indicators – KPI), de manera que se fortalezca la capacidad de seguimiento preventivo, facilitando la toma de decisiones y la implementación de acciones oportunas antes de que los riesgos se materialicen. De esta forma, el monitoreo trasciende la verificación de la eficacia de los controles y se orienta a la gestión proactiva de los riesgos mediante el análisis continuo de señales e indicadores asociados a los procesos institucionales.

En caso de contar con proyectos, cada Gerente de proyecto será el responsable de gestionar adecuadamente los riesgos asociados a este, y deberá establecer la periodicidad de monitoreo y seguimiento que considere pertinente.

Las responsabilidades en el marco de las líneas de aseguramiento se definen de la siguiente manera:

 Unidad de Planeación Minero Energética	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

- Línea Estratégica (Alta Dirección y Comité Institucional de Coordinación de Control Interno): Establece los lineamientos para la gestión integral del riesgo, promueve la cultura de gestión preventiva y supervisa periódicamente el comportamiento de los riesgos institucionales mediante el análisis de la información consolidada de los Indicadores Clave de Riesgo (KRI) y su articulación con los Indicadores Clave de Desempeño o de Proceso (KPI). Asimismo, evalúa la efectividad de las estrategias de tratamiento implementadas, toma decisiones frente a los riesgos que superen los niveles de tolerancia definidos y orienta la adopción de acciones de mejora para fortalecer la gestión del riesgo en la entidad.
- El Líder del Proceso, en su rol como primera línea de defensa, realiza la supervisión continua de los riesgos asociados a su proceso, garantizando la implementación y funcionamiento de los controles definidos para su reducción o mitigación, así como de las acciones de fortalecimiento establecidas como estrategias de tratamiento del riesgo residual. Adicionalmente, define, monitorea y analiza los Indicadores Clave de Riesgo (KRI) asociados a los riesgos bajo su responsabilidad, asegurando su articulación con los Indicadores Clave de Desempeño o de Proceso (KPI), con el fin de identificar oportunamente señales de alerta temprana y variaciones en la exposición al riesgo. De acuerdo con la periodicidad definida por la entidad para el monitoreo y seguimiento, el Líder del Proceso debe comunicar los resultados de la gestión del riesgo, incluyendo el comportamiento de los KRI, las desviaciones identificadas, las alertas generadas y las acciones implementadas para su tratamiento; asimismo, deberá suministrar las evidencias correspondientes de la ejecución de los controles y de las acciones complementarias adoptadas.
- La segunda línea de defensa, realiza el seguimiento y la verificación de la gestión de los riesgos institucionales, brindando acompañamiento metodológico a los procesos en la identificación, valoración, tratamiento y monitoreo de los riesgos. Asimismo, consolida y analiza la información relacionada con los Indicadores Clave de Riesgo (KRI), especialmente aquellos asociados a los riesgos de mayor criticidad, con el fin de identificar tendencias, generar alertas tempranas y formular recomendaciones a la primera línea de defensa y a la Alta Dirección (línea estratégica). De igual manera, presenta periódicamente a la Alta Dirección los resultados del monitoreo de los riesgos y el comportamiento de los KRI críticos, facilitando la toma de decisiones oportunas para el fortalecimiento de la gestión del riesgo institucional.

En el caso de los riesgos de Integridad Pública, estas actividades se desarrollarán en articulación con la Función de Cumplimiento del Sistema de Gestión de Riesgos de Integridad Pública (SIGRIP), conforme a las responsabilidades y lineamientos establecidos para dicha función.

- Control Interno, como tercera línea de defensa, a través de su proceso de auditoría interna, realiza evaluaciones independientes sobre la gestión integral de los riesgos, con el fin de determinar la efectividad de los controles establecidos para prevenir o mitigar la materialización de los riesgos y verificar la adecuada implementación de las políticas, procedimientos y metodologías definidas por la entidad.

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

Asimismo, evalúa la pertinencia y eficacia de los Indicadores Clave de Riesgo (KRI) definidos por los procesos, verificando que estos permitan generar alertas tempranas oportunas sobre cambios en la exposición al riesgo y apoyen la toma de decisiones preventivas. Como resultado de sus evaluaciones, formula recomendaciones orientadas al fortalecimiento del Sistema de Control Interno y de la gestión del riesgo, de conformidad con las responsabilidades propias de su rol como tercera línea de defensa.

5.3.3. Acciones Ante la Materialización de Riesgos (Gestión de Eventos)

Cuando un riesgo se materialice, el líder del proceso deberá informar de manera inmediata el evento, analizar sus causas, evaluar la efectividad de los controles implementados, definir y ejecutar las acciones correctivas, preventivas o de mejora correspondientes, actualizar el mapa de riesgos cuando aplique y realizar el seguimiento a las acciones definidas hasta su cierre. De igual manera, deberá garantizar la continuidad de la operación y el cumplimiento de los objetivos institucionales afectados por el evento materializado.

De manera específica, para cada tipología de riesgo se deberán considerar las siguientes acciones:

- **Riesgos de Gestión:** Identificar las causas de la materialización, revisar la efectividad de los controles existentes, implementar acciones correctivas y de mejora, actualizar la valoración del riesgo y efectuar seguimiento hasta verificar la mitigación de sus efectos.
- **Riesgos Fiscales:** Adoptar medidas inmediatas para evitar o limitar la ocurrencia de daño al patrimonio público, fortalecer los controles asociados a la gestión fiscal, documentar el evento y realizar el seguimiento correspondiente para prevenir su recurrencia. En caso de requerirse, se deberá informar a las instancias competentes conforme a la normatividad vigente. Basado en el enfoque preventivo de la gestión del riesgo fiscal desarrollado en la Guía.
- **Riesgos de Seguridad de la Información:** Gestionar el incidente de seguridad, contener y recuperar los activos de información afectados, restablecer la disponibilidad, integridad y confidencialidad de la información, implementar los controles requeridos y efectuar el reporte y seguimiento del evento de acuerdo con los lineamientos institucionales de seguridad de la información.
- **Riesgos para la Integridad Pública (incluyendo corrupción, fraude, soborno, conflictos de interés y LA/FT/FP):** Adoptar medidas para garantizar la continuidad de la prestación del servicio y de la operación institucional, implementar acciones de control y mitigación frente a los efectos generados, fortalecer los mecanismos de prevención, detección y monitoreo, y realizar los reportes a las instancias competentes cuando corresponda, sin que la gestión del riesgo implique por sí misma juicios de responsabilidad o sanciones.

Para el detalle de las actividades, responsables, tiempos de respuesta, mecanismos de reporte y tratamiento específicos aplicables a cada tipología de riesgo, se deberá consultar el procedimiento PRO-PES-003 Gestión Integral del Riesgo y los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas – en su última versión,

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

documentos que desarrollan de manera integral el tratamiento de eventos de riesgo materializados y las actuaciones que deben adelantar las diferentes líneas de defensa.

5.3.4. Información, Comunicación y Reporte

La comunicación y consulta son elementos transversales durante todas las etapas de la administración de riesgos. La comunicación busca promover la toma de conciencia y la comprensión del riesgo, e implica compartir información de forma oportuna y pertinente con todos los servidores públicos, contratistas y demás colaboradores que participen en el cumplimiento de los objetivos institucionales. Así mismo a terceros que suscriban con la UPME, convenios, alianzas u otros mecanismos de articulación institucional. La consulta implica que los participantes proporcionen retroalimentación e información que contribuya a la toma de decisiones. La comunicación y consulta implica actividades como:

- La promoción de la participación de los servidores públicos y contratistas, con el fin de que aporten su conocimiento en las diferentes etapas de la administración de riesgos.
- La permanente socialización de la política para la Gestión Integral de Riesgos en todos los niveles de la entidad es responsabilidad de las tres líneas de defensa, de acuerdo con el alcance de su rol, para que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una frente a la gestión del riesgo.
- Las capacitaciones, asesoramientos y acompañamientos para la implementación de la metodología, incluyendo explícitamente la toma de conciencia sobre los objetivos, beneficios y las implicaciones del incumplimiento del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP).
- Los informes con los resultados de las fases de identificación y descripción, análisis de riesgo inherente, diseño y análisis de controles, y valoración del riesgo residual.
- Los reportes e informes derivados de los monitoreos y seguimientos realizados por las tres líneas de defensa deberán incluir los resultados obtenidos en la gestión de los riesgos, el estado de los controles, las acciones implementadas y el comportamiento de los Indicadores Clave de Riesgo (KRI), así como el reporte oportuno de las alertas tempranas identificadas, con el fin de facilitar la toma de decisiones y la adopción de medidas preventivas para evitar o reducir la materialización de los riesgos.
- La difusión y promoción del canal institucional de denuncias por corrupción y el buzón ético, garantizando que todos los servidores y partes interesadas conozcan los mecanismos seguros para el reporte de operaciones inusuales o sospechosas (LA/FT/FP)
- Los reportes de información generados por control interno como tercera línea de defensa para los entes de control que lo requieran, en el marco de su rol de relación con entes externos.
- La comunicación externa orientada a difundir entre la ciudadanía y los grupos de valor los resultados de la gestión de riesgos y del Programa de Transparencia y Ética Pública, en el marco del enfoque de Estado Abierto y la rendición de cuentas.

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

5.3.5. Niveles de Responsabilidad y Autoridad Frente a la Administración del Riesgo en la Entidad (acorde con el esquema de líneas de defensa)

A continuación, en la **Tabla 3**, se describen los roles y responsabilidades acorde con el esquema de las líneas de defensa del modelo del MIPG:

Tabla 3 Roles y Responsabilidades en la Gestión de Riesgos - Líneas de Defensa

LÍNEA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
LÍNEA ESTRATÉGICA 	Alta Dirección y Comité Institucional de Gestión y Desempeño	Generar recomendaciones de mejora a la Política para la Gestión Integral de Riesgos para su análisis y actualización. Impulsar la implementación de la política, metodologías y mecanismos para la gestión de riesgos. Revisar y considerar los resultados presentados de los monitoreos y seguimientos, para la toma de decisiones. Revisar las actualizaciones presentadas de los mapas de riesgos, para brindar recomendaciones en el marco de la estrategia de la entidad. Definir, revisar y aprobar el apetito de riesgo de la entidad, entendiendo este como el nivel de riesgo que la UPME está dispuesta a aceptar para el logro de sus objetivos estratégicos y el cumplimiento de su misión institucional. El apetito de riesgo servirá como marco de referencia para la toma de decisiones, la gestión de los riesgos institucionales y la definición de estrategias de tratamiento y control. Asegurar la disponibilidad y asignación de los recursos humanos, técnicos, tecnológicos y financieros necesarios para la implementación, mantenimiento y mejora continua de la Política de Gestión Integral de Riesgos. Así mismo, deberá definir y comunicar las responsabilidades de las diferentes líneas de defensa y de los actores involucrados en la gestión de riesgos, garantizando su articulación con los objetivos institucionales, el Modelo Integrado de Planeación y Gestión (MIPG) y el Sistema de Control Interno. Analizar periódicamente los resultados de la gestión integral de riesgos y de la evaluación del Sistema de Control Interno, promoviendo la adopción de acciones de mejora que contribuyan al fortalecimiento de la capacidad institucional, el logro de los objetivos estratégicos y la generación y protección de valor público.
	Alta Dirección y Comité Institucional de Coordinación de Control Interno	Aprobar la Política Para la Gestión Integral de Riesgos previamente estructurada por parte de la Oficina Asesora de Planeación, como segunda línea de defensa en la entidad. Establecer las intenciones generales para hacer una adecuada gestión de los riesgos y comunicar lo que espera obtener de la operativización de la política integral de administración de riesgos. Analizar el seguimiento al cumplimiento de la Política Para la Gestión Integral de Riesgos. Establecer recomendaciones para los riesgos identificados, revisando que son pertinentes para entidad y se alinean con el contexto actual. Analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento del Plan Estratégico Institucional, para la toma de decisiones.
	Líderes y Enlaces de Procesos MIPG	Conocer y apropiar la política integral de administración de riesgos y el procedimiento "PRO-PES-003 Gestión Integral del Riesgo", con el propósito de tomar acciones para el autocontrol en sus procesos y promoverlo al interior de su equipo de trabajo. Identificar, valorar, evaluar, actualizar los riesgos, establecer los controles y garantizar su implementación, para evitar su materialización.

 Unidad de Planeación Minero Energética	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

LÍNEA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
LÍNEA ESTRATÉGICA 	Líderes y Enlaces de Procesos MIPG	Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar sus deficiencias y determinar las acciones de mejora a que haya lugar. Revisar y gestionar las acciones complementarias establecidas para apoyar el tratamiento de los riesgos materializados. Reportar los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. En caso de la materialización de un riesgo realizar su comunicación y respectivo tratamiento de acuerdo con las actividades del procedimiento de "PRO-PES-003 Gestión Integral del Riesgo". Solicitar a la Oficina Asesora de Planeación la eliminación de un riesgo con la debida justificación, para evaluar su pertinencia. Comunicar a la Oficina Asesora de Planeación la necesidad de la actualización de un riesgo, para realizar su debido acompañamiento. Comunicar al interior de sus equipos de trabajo, las actualizaciones de los mapas de riesgos, haciendo énfasis en los riesgos que son gestionados desde su proceso y los controles a los responsables de su ejecución. Comunicar al interior de sus equipos de trabajo, los informes con los resultados de la gestión de riesgos y atender las recomendaciones brindadas para su definición, implementación o mejora.
	Servidores Públicos y Contratistas	Conocer y apropiarse la política integral de administración de riesgos y el procedimiento de "PRO-PES-003 Gestión Integral del Riesgo", tomando acciones para el autocontrol en sus procesos. Participar en el diseño de los controles que tienen a cargo. Ejecutar los controles a su cargo de la forma como están diseñados. Informar al Líder del Proceso la materialización de riesgos o posibles situaciones de afectación al proceso, con el fin de incorporar las acciones a que haya lugar. Informar al Líder del Proceso sobre los eventos que, en el ejercicio de su función, puedan conllevar a la identificación de nuevos riesgos. Proponer mejoras a los controles existentes. Ejecutar las acciones complementarias o de mejora a su cargo asociadas a la gestión de riesgos.
SEGUNDA LÍNEA DE DEFENSA 	Oficina Asesora de Planeación	Estructurar la política integral de administración de riesgos de acuerdo con lo definido en la "Guía para la Gestión Integral del Riesgo en Entidades Públicas". Presentar en el Comité Institucional de Coordinación de Control Interno necesidades de actualización de la política integral de administración de riesgos, para su aprobación. Proporcionar información del contexto interno y externo de la entidad, para la identificación de los riesgos. Acompañar, orientar y entrenar a los Líderes de Procesos y sus equipos en la identificación, análisis, valoración y evaluación del riesgo. Asesorar el adecuado diseño de los controles de acuerdo con lo indicado en la guía del DAFP. La Oficina Asesora de Planeación realiza la explicación del funcionamiento del sistema mediante mesas de trabajo o guías de apoyo. Al identificar eventos que no se encuentren dentro del mapa de riesgos, realizar mesas de trabajo con el proceso involucrado para su inclusión y gestión. Publicar y socializar las actualizaciones de la política integral de administración de riesgos y los mapas de riesgos. Hacer seguimiento a los controles establecidos, con la información suministrada por los Líderes de Procesos y enlaces de MIPG (primera línea de defensa) en los monitoreos. Asesorar la formulación de las acciones complementarias o de mejora que apoyan el tratamiento de los riesgos.

Página 17 de 22

 Unidad de Planeación Minero Energética	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

LÍNEA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
SEGUNDA LÍNEA DE DEFENSA 		Realizar el seguimiento y verificación a la gestión de los riesgos, estableciendo alertas y recomendaciones en relación. Evaluar la implementación del cumplimiento de la política integral de administración de riesgos y presentar la respectiva información consolidada. Establecer recomendaciones y alertas para la línea estratégica sobre eventos y cambios en el entorno, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos. Informar a la Dirección General y a Control Interno sobre las actualizaciones de riesgos o la eliminación justificada de riesgos. Trabajar de forma coordinada y articulada con la Dirección General y Control Interno en el fortalecimiento del Sistema de Control Interno. Reportar en el Comité Institucional de Coordinación de Control Interno las subsanaciones a las observaciones, oportunidades de mejora, recomendaciones y consideraciones relacionadas en los informes de auditoría de seguimiento a los riesgos.
	Oficina de Tecnologías de la Información	Monitorear el Plan Estratégico de Tecnologías de la Información – PETI y sus componentes, generando alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas en materia de tecnología y reportar en el Comité de Gestión y Desempeño Institucional.
	Oficial de Seguridad de la Información o Quien Haga sus Veces	Formular la metodología para la gestión de riesgos de seguridad y privacidad de la información establecida por la entidad, considerando la "Guía para la Gestión Integral del Riesgo en Entidades Públicas". Proponer la formulación de políticas y lineamientos de seguridad y privacidad de la información. Evaluar el cumplimiento de los controles asociados a las Políticas de Seguridad de la Información. Definir e implementar en coordinación con las dependencias de la entidad, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para servidores públicos y contratistas. Actualizar el procedimiento para la identificación y valoración de los Activos de la Entidad, de acuerdo con los criterios de seguridad de la información (confidencialidad, integridad y disponibilidad). Adoptar o actualizar el procedimiento formal para la gestión de riesgos de seguridad de la información (identificación, análisis, evaluación y tratamiento). Liderar, asesorar y acompañar a la primera línea de defensa en la gestión de riesgos de seguridad de la información, emitiendo recomendaciones de controles para prevenir o mitigar los riesgos. Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos de acuerdo con la periodicidad definida. Apoyar a los procesos de la entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información. Definir, socializar e implementar el procedimiento de Gestión de Incidentes de seguridad de la información en la entidad. Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información. Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los Líderes de los Procesos en seguridad y privacidad de la información. Poner en conocimiento de las dependencias con competencia funcional cuando se detecten irregularidades, incidentes o prácticas

Página 18 de 22

 Unidad de Planeación Minero Energética	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

LÍNEA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
SEGUNDA LÍNEA DE DEFENSA 	Oficial de Seguridad de la Información o Quien Haga sus Veces	que atenten contra la seguridad y privacidad de la información de acuerdo con la normativa vigente. Fomentar la implementación de la Política de Gobierno Digital. Asesorar a la entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y privacidad de la Información para la entidad de conformidad con la regulación vigente. Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación actual de la entidad. Realizar la estimación, planificación y cronograma de la implementación del MSPI. Liderar la implementación y hacer seguimiento a las tareas y cronograma definido. Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del MSPI. De acuerdo con las solicitudes realizadas por los proyectos o procesos, realizar el acompañamiento correspondiente en materia de seguridad y privacidad de la información.
	Oficial de protección de datos personales	Promover la elaboración, implementación y mantenimiento de mecanismos que permitan administrar los riesgos asociados al tratamiento de datos personales. Asesorar a los responsables y encargados del tratamiento y a los procesos de la Entidad en la identificación, análisis y gestión de los riesgos relacionados con la protección de datos personales. Analizar y verificar la conformidad de las actividades de tratamiento de datos personales y emitir las recomendaciones que correspondan. Realizar seguimiento a la implementación y funcionamiento del mecanismo definido para la Gestión de Datos Personales, incluyendo la evaluación y revisión periódica de sus controles. Articular con los líderes de proceso y demás instancias competentes las acciones necesarias para el tratamiento de los riesgos relacionados con la privacidad y protección de datos personales. Informar y formular recomendaciones frente a desviaciones, debilidades de control o situaciones que puedan afectar el adecuado tratamiento y protección de los datos personales.
	Secretaría General y GIT de Gestión Contractual	Monitorear la gestión contractual y generar alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas.
	GIT de Gestión Documental, Archivo y Servicio al Ciudadano	Monitorear las PQRSDF generando alertas sobre incumplimientos, quejas en la prestación del servicio, tutelas u otras situaciones de riesgo detectadas.
	GIT de Gestión de Talento Humano	Monitorear temas clave del ciclo del servidor (ingreso, desarrollo y retiro), generando alertas sobre incumplimientos, situaciones críticas que afectan en clima laboral y posibles afectaciones al código de integridad u otras situaciones de riesgo detectadas.
	Oficina Asesora Jurídica	Identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico, y realizar su monitoreo.

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

LÍNEA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
TERCERA LÍNEA DE DEFENSA 	Control Interno	Asesorar y orientar técnicamente y realizar recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación, para garantizar el cumplimiento efectivo de los objetivos. Monitorear la exposición de la entidad al riesgo y realizar recomendaciones con alcance preventivo. Asesorar de forma proactiva y estratégicamente a la Alta Dirección y los Líderes de Proceso y enlaces de MIPG, sobre las responsabilidades en materia de riesgos. Informar los hallazgos en materias de riesgos y proporcionar recomendaciones en el ejercicio de la auditoría independiente. Realizar seguimiento a los riesgos y remitir observaciones, oportunidades de mejora, recomendaciones y consideraciones sobre la pertinencia y efectividad de los controles. Promover los ejercicios de autoevaluación por parte de la primera línea de defensa, para definir la efectividad de los controles y el tratamiento de los riesgos. Formular recomendaciones y brindar orientación a la primera línea de defensa de forma coordinada con la segunda línea de defensa, en la mejora del diseño de controles. Realizar evaluación independiente de la gestión de los riesgos. Evaluar fallas en los controles (diseño y ejecución) para definir las acciones apropiadas para su mejora. Comunicar aquellos aspectos que consideren una amenaza para el cumplimiento de los objetivos de los procesos, de los objetivos y metas institucionales, en el marco de la evaluación independiente. Identificar y alertar al Comité Institucional de Coordinación de Control Interno de posibles cambios que pueden afectar la evaluación y el tratamiento del riesgo. Trabajar de forma coordinada con la Oficina Asesora de Planeación en el fortalecimiento del Sistema de Control Interno. Alertar sobre la probabilidad de riesgo de gestión, riesgos de posibles actos de corrupción, riesgos de seguridad de la información y riesgos fiscales.

Fuente: Elaboración OAP

La gestión integral de los riesgos en la UPME se desarrolla bajo el esquema de líneas de defensa, en el que cada instancia ejerce responsabilidades diferenciadas y complementarias frente al riesgo. La articulación entre la Línea Estratégica, la Primera Línea de Defensa, la Segunda Línea de Defensa y la Tercera Línea de Defensa fortalece la toma de decisiones, promueve una gestión preventiva basada en riesgos y contribuye al cumplimiento de los objetivos institucionales.

Para la aplicación de esta metodología, la entidad utilizará el sistema de información que determine para la administración y seguimiento de los riesgos, garantizando la trazabilidad, disponibilidad y oportunidad de la información requerida para su gestión. Asimismo, la UPME definirá, de acuerdo con sus necesidades y las particularidades de cada tipología de riesgo, los formatos, herramientas y mecanismos de registro que conformarán los mapas de riesgos y demás instrumentos de gestión, asegurando su alineación con la normatividad vigente y las mejores prácticas en materia de administración del riesgo.

6. ACTUALIZACIÓN

La Oficina Asesora de Planeación en su rol de segunda línea de defensa será responsable de coordinar la revisión, actualización, divulgación y socialización de la Política para la

Página 20 de 22

	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

Gestión Integral de Riesgos y sus actualizaciones, una vez estas sean aprobadas por la Alta Dirección a través del Comité Institucional de Coordinación de Control Interno.

Así mismo, la Política para la Gestión Integral de Riesgos y sus actualizaciones estarán disponibles para consulta permanente en los medios definidos por la entidad, con el fin de promover la transparencia, la cultura de gestión de riesgos y la participación informada de las partes interesadas.

7. COMUNICACIÓN Y DIVULGACIÓN

Para garantizar el conocimiento, la toma de conciencia y apropiación de la política por parte de los grupos de valor internos y externos, la entidad empleará mecanismos de comunicación y divulgación tales como la publicación bajo el enfoque de Estado Abierto, garantizando la transparencia activa y pasiva.

Para ello, se utilizarán canales de comunicación tales como la publicación permanente en el portal web institucional, la Intranet, correos electrónicos institucionales, jornadas de socialización, capacitaciones, mesas de trabajo, piezas comunicativas y demás canales institucionales que se consideren pertinentes.

A través de estos medios, la UPME promoverá el diálogo, la corresponsabilidad, la rendición de cuentas y el control social ciudadano, asegurando que se difundan oportunamente los resultados de la gestión de riesgos y los elementos del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), lo anterior alineado con definido en el Programa de Transparencia y Ética Pública (PTEP) de la Entidad.

8. ANEXOS

- Guía para la Gestión Integral del Riesgo en Entidades Públicas en su última versión
- Manual Operativo MIPG.

9. DOCUMENTOS RELACIONADOS

- Procedimiento PRO-PES-003 Gestión Integral del Riesgo.
- Procedimiento PRO-SPI-001 Gestión de Riesgos de Seguridad de la Información.
- Procedimiento PRO-MCO-003 Acciones Correctivas, de Mejora y Para Abordar Riesgos
- Política POL-EYC-002 Administración y Gestión del Riesgo de LA/FT/FP

10. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
Fecha	Versión	Descripción de los cambios
07/11/2025	1	En el mapa de procesos MP-01 V3, esta política se encontraba vinculada al proceso de Direccionamiento Estratégico, procedimiento L-DE-001.
		Se efectúa ajuste de la política integral de

 Unidad de Planeación Minero Energética	POLÍTICA INSTITUCIONAL PARA LA GESTIÓN INTEGRAL DE RIESGOS	Código: POL-EYC-001
		Fecha: 02/10/2026
		Versión: 01

		administración de riesgos, de acuerdo con las intenciones generales de la Alta Dirección para hacer una adecuada gestión de los riesgos. Se vincula en versión 1 al proceso de Planeación Estratégica.
XX/06/2026	1 Es versión 1 dado que cambia de proceso responsable	Se incorporan los nuevos lineamientos emitidos por el Departamento Administrativo de la Función Pública (DAFP), en el marco del Sistema de Gestión de Riesgos para la Integridad Pública, contenidos en la versión 7 de la Guía para la Gestión Integral del Riesgo en Entidades Públicas. Se modifica nombre del procedimiento a: Política Institucional para la gestión Integral de Riesgos y se traslada la política al proceso de Evaluación y Control ahora POL-EYC-001 v1 anterior POL-PES-001 Política Integral de Administración de Riesgos - UPME Se realiza aprobación de las modificaciones a la política en el Comité Institucional de Coordinación de Control Interno No 01 del 17/09/2026

ELABORÓ	REVISÓ	APROBÓ
Nombre: Luisa Fernanda Sánchez Gómez Cargo: Contratista – Oficina Asesora de Planeación. Fecha: 17/06/2026	Nombre: Mónica Julieth Ovalle Rey Cargo: Profesional Universitario Oficina Asesora de Planeación Fecha: 13/08/2026	Nombre: María Carolina Obando Vargas Cargo: Líder de la Política Jefe Oficina Asesora de Planeación (E) Fecha: 14/09/2026 Comité Institucional de Coordinación de control Interno No 01 Fecha: 17/09/2026