

## POLÍTICA DE ADMINISTRACIÓN DE RIESGOS – UPME

### 1. INTRODUCCIÓN

El presente documento establece la Política de Administración de Riesgos de la Unidad de Planeación Minero Energética – UPME. Así como, los lineamientos para la identificación, y valoración de los riesgos que puedan afectar el cumplimiento de la misión, de los objetivos estratégicos, la gestión de los procesos y la satisfacción de los grupos de interés, de acuerdo con las directrices del Modelo Integrado de Planeación y Gestión- MIPG, la responsabilidad de la línea estratégica y líneas de defensa definidas en el Modelo Estándar de Control Interno – MECI – Dimensión 7 Control Interno y la Guía para la administración del riesgo expedida por el Departamento Administrativo de la Función Pública.

### DECLARACIÓN POLÍTICA PARA LA ADMINISTRACIÓN DE RIESGOS DE LA UPME

La Alta Dirección de la UPME y el equipo humano de la entidad está comprometido para llevar a cabo una gestión integral de riesgos que facilite el cumplimiento de la misión, los objetivos estratégicos, objetivos de los procesos y la satisfacción de los grupos de interés, llevando a cabo la identificación de riesgos de gestión por proceso, los riesgos de corrupción y los riesgos de seguridad digital, su análisis, valoración y formulación de los planes de tratamiento de riesgos o acciones para prevenir su ocurrencia o mitigar el impacto.

Las políticas de manejo de riesgo aplican a todos los procesos de la UPME y establecen las opciones para el tratamiento de los riesgos. Los riesgos de corrupción son inaceptables y en consecuencia no se pueden asumir. El tratamiento general para los riesgos corresponde a la implementación de acciones que conlleven a reducir, evitar, compartir, aceptar o transferir y serán individuales para cada uno de los riesgos identificados. Las acciones o controles se formularán considerando su viabilidad técnica, económica y legal.

Los procedimientos de: Gestión Integral de Riesgos P-DE-07 y P-TI-03 Seguridad de la información, hacen parte integral de la presente política y en ellos se establece los niveles de aceptación del riesgo, niveles para calificar la probabilidad y el impacto, tratamiento de riesgos, periodicidad de seguimiento y demás aspectos metodológicos.

### 1. OBJETIVO GENERAL

Establecer los lineamientos para la administración de los riesgos de gestión, corrupción y seguridad digital asociados a la gestión institucional.

#### 1.1. OBJETIVOS ESPECÍFICOS

- Comunicar a todos los niveles de la Unidad los lineamientos para la administración del riesgo, para promover su aplicación.
- Fomentar la cultura de la prevención del riesgo en todos los niveles de la Institución.

- Asignar responsabilidades frente a la administración del riesgo.

### 3. ALCANCE

La Política para la Administración de Riesgos es aplicable a todos los procesos del Sistema de Gestión de la Unidad, así como a todas las dependencias y niveles.

Los riesgos de Gestión por proceso y de Corrupción, se establecerán de acuerdo con los lineamientos que emita el Departamento Administrativo de la Función Pública – DAFP, a través de la guía de riesgos.

Los riesgos del Sistema de Seguridad y Salud en el Trabajo, Seguridad digital y los riesgos del Sistema de Gestión Ambiental, se establecerán de acuerdo con la normatividad aplicable en cada caso.

### 4. TÉRMINOS Y DEFINICIONES

**DAFP:** Departamento Administrativo de la Función Pública.

**Política de administración del riesgo:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del Riesgo.

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

Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

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

**Riesgo de Seguridad Digital:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

### 5. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

La administración del riesgo depende de la participación de la Alta dirección, servidores públicos y contratistas; por esto se deben identificar las responsabilidades de acuerdo con los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión - MIPG, a partir de la estructuración de las líneas de defensa que se presentan a continuación:

Tabla No.1: Líneas de Defensa Frente a la Responsabilidad de los Riesgos en la UPME

LÍNEA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
<b>LÍNEA ESTRATÉGICA</b>	Comité Institucional de Coordinación de Control Interno	<ul style="list-style-type: none"> <li>Definir y aprobar la política para la administración del riesgo</li> <li>Analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento del plan estratégico</li> <li>Analizar los riesgos, vulnerabilidades, amenazas que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad, gestión de los procesos y capacidades para prestar servicios.</li> <li>Monitorear el cumplimiento de la política de administración de riesgo de la entidad</li> </ul>
	Comité de Gestión y Desempeño Institucional	<ul style="list-style-type: none"> <li>Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo).</li> <li>Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles.</li> </ul>
<b>PRIMERA LÍNEA DE DEFENSA</b>	Líderes de Proceso	<ul style="list-style-type: none"> <li>Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a los procesos.</li> <li>Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión.</li> <li>Ejecutar y supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar.</li> <li>Informar al GIT de Planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo.</li> <li>Reportar los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.</li> </ul>
	Secretaria General Subdirectores (as)  Jefes de Oficina  Responsable de proyecto	
<b>SEGUNDA LÍNEA DE DEFENSA</b>	GIT de Planeación	<ul style="list-style-type: none"> <li>Asesorar a la línea estratégica en la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual.</li> <li>Consolidar el mapa de riesgos y presentarlo para análisis y seguimiento ante el Comité Institucional de Coordinación de Control Interno</li> <li>Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo.</li> <li>Asegurar que los controles y acciones de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente.</li> </ul>

LÍNEA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
		<ul style="list-style-type: none"> <li>• Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos.</li> <li>• Evaluar que la gestión de los riesgos esté acorde con la presente política y que sean monitoreados por la primera línea de defensa.</li> <li>• Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles para el tratamiento de los riesgos.</li> <li>• Generar reportes periódicamente al Comité Institucional de Coordinación de Control Interno y al Comité institucional de Gestión y Desempeño acerca del cumplimiento de las metas y los objetivos en relación a la gestión integral del riesgo.</li> </ul>
<b>SEGUNDA LÍNEA DE DEFENSA</b>	Coordinadores GIT: Administrativa, Financiera, Talento Humano y Servicio al Ciudadano  GIT de Gestión Jurídica y Contractual  Comité de contratación  Delegados de riesgos en cada proceso	<ul style="list-style-type: none"> <li>• Acompañar a los líderes de procesos en la identificación, análisis, valoración, evaluación del riesgo, la definición de controles bajo su responsabilidad y los temas a su cargo.</li> <li>• Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo.</li> <li>• Realizar el seguimiento al mapa de riesgos de su proceso.</li> <li>• Reportar los avances de la gestión del riesgo.</li> <li>• Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo.</li> <li>• Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su proceso o responsabilidad.</li> <li>• Identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico bajo responsabilidad del GIT de Gestión Jurídica y Contractual o quien haga sus veces.</li> <li>• Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo</li> </ul>
<b>SEGUNDA LÍNEA DE DEFENSA</b>	Jefe o profesional de la OGI quien desempeñe el rol de Oficial de Seguridad de la Información	<ul style="list-style-type: none"> <li>• Liderar y coordinar la implementación de las políticas de Seguridad de la Información, con la participación activa de las dependencias de la entidad.</li> <li>• Evaluar y coordinar la implementación de controles específicos de Seguridad de la Información para sistemas de información o servicios informáticos.</li> <li>• Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.</li> <li>• Identificar las necesidades y recursos necesarios (tecnológicos, humanos, de capacitación, financieros, etc.) para el mantenimiento de la infraestructura de Seguridad de la Información.</li> <li>• Identificar las necesidades de formación (capacitación y entrenamiento) del Comité Institucional de Gestión y</li> </ul>

LÍNEA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
		<p>Desempeño, y establecer un plan de capacitación para formar y entrenar a sus integrantes.</p> <ul style="list-style-type: none"> <li>● Actuar como asesor en Seguridad de la Información para la entidad.</li> <li>● Realizar seguimiento al comportamiento de los indicadores de gestión de la Seguridad de la Información que apruebe el Comité Institucional de Gestión y Desempeño.</li> <li>● Realizar la evaluación del desempeño del SGSI</li> <li>● Realizar la revisión y supervisión del SGSI</li> <li>● Establecer un programa periódico (por lo menos una vez al año) de revisión de vulnerabilidades de la plataforma tecnológica de la entidad y coordinar los respectivos aseguramientos conforme los resultados de las mencionadas pruebas.</li> <li>● Reportar al Comité Institucional de Gestión y Desempeño el estado de la investigación y monitoreo de los incidentes de Seguridad de la Información, los resultados de las auditorías periódicas, la revisión y supervisión del SGSI.</li> <li>● Presentar al Comité Institucional de Gestión y Desempeño iniciativas e informes periódicos del estado de Seguridad de la Información de la entidad.</li> <li>● Identificar los organismos externos que ejerzan autoridad en lo relacionado con los aspectos de Seguridad de la Información e identificar los mecanismos de contacto respectivos. Al menos se debe identificar el contacto con las siguientes autoridades: Grupo Investigativo Delitos Informáticos (DEINF) de la DIJIN, Unidad de delitos Informáticos de la Fiscalía General de la Nación, COLCERT, CCOC, CCP, CSIRT.</li> <li>● Identificar comunidades y grupos de interés relacionados con Seguridad de la Información que le permitan mantenerse actualizado y en contacto con expertos en los temas de Seguridad.</li> <li>● Rendir ante el Comité Institucional de Gestión y Desempeño informes durante los primeros quince (15) días de cada trimestre, precisando el estado y avance de la implementación del Sistema de Gestión de Seguridad de la Información y sus políticas.</li> <li>● Definir el procedimiento para la Identificación y Valoración de Activos.</li> <li>● Adoptar o adecuar el procedimiento formal para la gestión de riesgos de Seguridad Digital (Identificación, Análisis, Evaluación y Tratamiento).</li> <li>● Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de Seguridad Digital y en la recomendación de controles para mitigar los riesgos.</li> <li>● Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.</li> </ul>

LÍNEA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
		<ul style="list-style-type: none"> <li>• Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de Seguridad Digital.</li> </ul>
<b>TERCERA LÍNEA DE DEFENSA</b>	Asesor de Control Interno	<ul style="list-style-type: none"> <li>• Brindar asesoría, orientación técnica, evaluación y seguimiento a la gestión del riesgo</li> <li>• Brindar asesoría a los responsables y ejecutores de los procesos y proyectos (primera línea de defensa), respecto a metodologías y herramientas para la identificación, análisis y evaluación de riesgos, como complemento a la labor de acompañamiento que debe desarrollar la segunda línea de defensa.</li> <li>• Asesorar a la primera línea de defensa de forma coordinada con la segunda línea de defensa, en la identificación de los riesgos y diseño de controles.</li> <li>• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.</li> <li>• Pronunciarse sobre la pertinencia y efectividad de los controles</li> <li>• Recomendar mejoras a la política de operación para la administración del riesgo</li> <li>• Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa.</li> <li>• Señalar 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.</li> <li>• Identificar y alertar al Comité de Coordinación de Control Interno posibles cambios que pueden afectar la evaluación y el tratamiento del riesgo.</li> </ul>

Fuente: Guía de Riesgos adoptado del MIPG- DAFP y adaptado por el GIT de Planeación de la UPME

De igual manera, el Coordinador o Coordinadora del GIT de Planeación llevará a cabo las siguientes acciones:

- Socializar anualmente la metodología de riesgos.
- Capacitar al grupo de trabajo de cada dependencia en la herramienta SIGUEME para la gestión del riesgo.
- Liderar las mesas de trabajo de identificación del riesgo.
- Socializar y publicar el mapa de riesgos de gestión y de corrupción.
- Publicar los mapas de riesgos de seguridad digital.

Por su parte, los líderes de proceso tienen la responsabilidad de:

- Asegurar que al interior de su grupo de trabajo se reconozca el concepto de “administración del riesgo”, la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa.

- Delegar, por parte del líder del proceso, el (los) profesionales que se encargarán del monitoreo, reporte y socialización del riesgo asociados.

Así mismo el Jefe o profesional de la OGI con rol de Oficial de Seguridad de la Información tiene responsabilidad de:

- Informar a la línea estratégica sobre los resultados de los análisis de riesgos de Seguridad Digital en cada uno de los procesos.
- Socializar y publicar los mapas de riesgos de seguridad digital.
- Liderar las mesas de trabajo de identificación del riesgo de seguridad digital.

Todos los servidores tienen la responsabilidad de ejecutar controles operativos en sus labores cotidianas y generar las alertas cuando identifiquen situaciones anómalas en esta ejecución.

## 6. ETAPAS PARA LA GESTIÓN DEL RIESGO

La gestión de riesgos comprende las actividades de análisis del contexto interno y externo, identificación, valoración y definición de controles para el tratamiento y seguimiento.

Las diferentes etapas del Componente de Seguridad Digital se describen en el Procedimiento Gestión integral del Riesgo Código P-DE-07 y Procedimiento de Gestión de Riesgos de Seguridad Digital P-TI-03. Estos lineamientos se basarán en la Guía para la administración del riesgo expedido por el DAFP.

## CONTROL DE CAMBIOS

FECHA	VERSIÓN	MOTIVO DE CAMBIO
19 de junio de 2021	1	Se incluyó Objetivos específicos, matriz de responsabilidades de líneas de defensa y se realizó revisión y ajuste general del documento. Se realizó revisión general de acuerdo con la Guía del DAFP
09 de noviembre de 2021	2	Se incluye en la Política Integral el componente de Seguridad Digital. Se eliminan definiciones o se ajustan de acuerdo con la guía del DAFP versión 5. Se eliminan aspectos metodológicos para integrarlos en el procedimiento de Gestión integral el Riesgo y el procedimiento de Gestión de Riesgos de Seguridad Digital y evitar duplicidad