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.

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

A continuación, se relacionan algunos de los conceptos, necesarios para la comprensión de la metodología señalados por el DAFP.

Activo de Información: Un activo es cualquier elemento que tenga valor para la entidad, en el contexto de seguridad digital son activos elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información - TI- o Tecnologías de la Operación -TO- que utiliza la entidad para su funcionamiento.

Administración de Riesgos: Es el proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar un aseguramiento razonable con respecto al logro de los objetivos. Incluye el conjunto de elementos de control y sus interrelaciones, para que la UPME maneje los eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos institucionales. La Administración del riesgo contribuye a generar la cultura de autocontrol y autoevaluación al interior de la Unidad.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de Riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo

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.

Contexto Interno: Es el entorno interno en el cual la organización busca definir y lograr sus objetivos

Contexto Externo. Es el entorno externo en el cual la organización busca definir y lograr sus objetivos

Control: Medida que permite reducir o mitigar un riesgo. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

DAFP: Departamento Administrativo de la Función Pública.

Evaluación del Riesgo: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Presencia o cambio de un conjunto particular de circunstancias.

Gestión del Riesgo: Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo.

Identificación del Riesgo: Proceso para encontrar, reconocer y describir el riesgo.

Impacto: Son las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Monitoreo: Verificación, supervisión, observación crítica o determinación continúa del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

Nivel o Zona del Riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Plan para el Tratamiento o Gestión del Riesgo: Conjunto de acciones preventivas que se encuentran dentro del marco de referencia para gestionar los riesgos, en esta se definen componentes como los responsables, los recursos y los métodos que se van a utilizar para mitigar, eliminar o asumir los riesgos.

Política de Operación: Aquella directriz general que reconoce el marco legal que rige y aplica a la UPME y la cual es desarrollada a través de la definición de los procesos, los procedimientos y las guías internas, que involucran las líneas de acción, los objetivos, actividades, tareas y controles que permiten el logro del objeto misional de la entidad y el cumplimiento de las responsabilidades con el estado.

Política de administración del riesgo: Declaración de la entidad e intenciones generales de la organización con respecto a la gestión del Riesgo.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Revisión: Acción que se emprende para determinar la idoneidad, conveniencia y eficacia de la materia en cuestión para lograr los objetivos establecidos.

Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso.

Riesgo Aceptable: Riesgo que ha sido reducido a un nivel que la organización puede tolerar con respecto a sus obligaciones legales.

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

Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgo Inherente: Es aquel al que se enfrenta una entidad en ausencia en acciones de la dirección para modificar su probabilidad e impacto.

Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgos Operativos: Comprende riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

Riesgo Residual: Riesgo remanente después del tratamiento del riesgo. Es el riesgo que permanece después de que la dirección haya realizado sus acciones para reducir el impacto y la probabilidad de un acontecimiento adverso, incluyendo las actividades de control en respuesta a un riesgo.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

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.

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

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
LÍNEA ESTRATÉGICA	Comité Institucional de Coordinación de Control Interno	● Definir y aprobar la política para la administración del riesgo ● Analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento del plan estratégico ● 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. ● Monitorear el cumplimiento de la política de administración de riesgo de la entidad
	Comité de Gestión y Desempeño Institucional	● Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo). ● Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles.
PRIMERA LÍNEA DE DEFENSA	Líderes de Proceso Secretaria General	● Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a los procesos. ● Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. ● Ejecutar y supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día

	Subdirectores (as) Jefes de Oficina Responsable de proyecto	a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. ● Informar al GIT de Planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo. ● Reportar los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.
SEGUNDA LÍNEA DE DEFENSA	GIT de Planeación	● 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. ● Consolidar el mapa de riesgos y presentarlo para análisis y seguimiento ante el Comité Institucional de Coordinación de Control Interno ● Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. ● Asegurar que los controles y acciones de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente. ● Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. ● Evaluar que la gestión de los riesgos esté acorde con la presente política y que sean monitoreados por la primera línea de defensa. ● Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles para el tratamiento de los riesgos. ● 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.
SEGUNDA LÍNEA DE DEFENSA	Coordinadores GIT: Administrativa, Financiera, Talento Humano y Servicio al Ciudadano, GIT de Gestión Jurídica y Contractual. Comité de contratación	● 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. ● Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. ● Realizar el seguimiento al mapa de riesgos de su proceso. ● Reportar los avances de la gestión del riesgo. ● Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. ● Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su proceso o responsabilidad. ● Identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico bajo responsabilidad

	Delegados de riesgos en cada proceso	del GIT de Gestión Jurídica y Contractual o quien haga sus veces. ● Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo
SEGUNDA LÍNEA DE DEFENSA	Jefe o profesional de la OGI quien desempeñe el rol de Oficial de Seguridad de la Información	● Liderar y coordinar la implementación de las políticas de Seguridad de la Información, con la participación activa de las dependencias de la entidad. ● Evaluar y coordinar la implementación de controles específicos de Seguridad de la Información para sistemas de información o servicios informáticos. ● Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes. ● Identificar las necesidades y recursos necesarios (tecnológicos, humanos, de capacitación, financieros, etc.) para el mantenimiento de la infraestructura de Seguridad de la Información. ● Identificar las necesidades de formación (capacitación y entrenamiento) del Comité Institucional de Gestión y Desempeño, y establecer un plan de capacitación para formar y entrenar a sus integrantes. ● Actuar como asesor en Seguridad de la Información para la entidad. ● Realizar seguimiento al comportamiento de los indicadores de gestión de la Seguridad de la Información que apruebe el Comité Institucional de Gestión y Desempeño. ● Realizar la evaluación del desempeño del SGSI ● Realizar la revisión y supervisión del SGSI ● 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. ● 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. ● Presentar al Comité Institucional de Gestión y Desempeño iniciativas e informes periódicos del estado de Seguridad de la Información de la entidad. ● 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. ● 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.

		● 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. ● Definir el procedimiento para la Identificación y Valoración de Activos. ● Adoptar o adecuar el procedimiento formal para la gestión de riesgos de Seguridad Digital (Identificación, Análisis, Evaluación y Tratamiento). ● 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. ● Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos. ● Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de Seguridad Digital.
TERCERA LÍNEA DE DEFENSA	Asesor de Control Interno	● Brindar asesoría, orientación técnica, evaluación y seguimiento a la gestión del riesgo ● 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. ● 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. ● 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. ● Pronunciarse sobre la pertinencia y efectividad de los controles ● Recomendar mejoras a la política de operación para la administración del riesgo ● Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. ● 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. ● Identificar y alertar al Comité de Coordinación de Control Interno posibles cambios que pueden afectar la evaluación y el tratamiento del riesgo.

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 de Gestión de Riesgos de Seguridad Digital P-TI-03(En proceso de creación) Estos lineamientos se basarán en la Guía para la administración del riesgo expedido por el DAFP.

7. NIVELES DE ACEPTACIÓN AL RIESGO

Los niveles de aceptación del riesgo se determinan como resultado de la valoración de la probabilidad de ocurrencia del riesgo y de la magnitud del impacto al momento de evaluar su materialización. Los riesgos de gestión inherentes, ubicados en la zona de riesgos "baja" pueden ser aceptados y por lo tanto no es necesario establecer controles. Los riesgos de corrupción son los únicos que son inaceptables en todo sentido, por tanto, deben tener controles permanentes y realizar su seguimiento.

El mapa de calor de riesgos permite visualizar los riesgos de gestión en las zonas de riesgos definidas (Baja, Moderada, Alta, Extremo) permitiendo identificar y priorizar los riesgos asociados a su gestión que requieren mayor atención, así como los que está dispuesta a

buscar o retener (apetito del riesgo) en función del impacto de estos en la Unidad. Los riesgos que se encuentren en zona baja se aceptan y se continúa el monitoreo.

El mapa de calor de riesgos permite visualizar los riesgos de seguridad digital en las zonas de riesgos definidas (Bajo, Moderado, Alto, Extremo) permitiendo identificar y priorizar los riesgos asociados a su gestión que requieren mayor atención; estableciendo un plan de gestión de riesgos de seguridad digital en el cual se identifiquen las amenazas, las vulnerabilidades, el impacto y el nivel de riesgo asociado a los activos de información sin importar el nivel de criticidad que tienen para la entidad. Los riesgos de seguridad digital que se encuentren en las zonas Bajo y Moderado se aceptan y se continúa el monitoreo.

Los riesgos de corrupción no admiten la aceptación del riesgo, siempre deben conducir a un tratamiento. Los riesgos que se encuentran en las zonas más altas son los que se priorizan orientando los esfuerzos y acciones para mejorar su administración de riesgos.

8. NIVELES PARA CALIFICAR EL IMPACTO.

Las tablas de calificación del impacto definidas para los Riesgos de Gestión, Corrupción y Seguridad Digital se definen así:

Tabla 2. Criterios para calificar la probabilidad y el impacto de los riesgos de gestión - Probabilidad

Frecuencia	Nivel	Descriptor	Descripción
Más de 1 vez al año.	5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.
Al menos 1 vez en el último año.	4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.
Al menos 1 vez en los últimos 2 años.	3	Posible	El evento podrá ocurrir en algún momento.
Al menos 1 vez en los últimos 5 años.	2	Improbable	El evento puede ocurrir en algún momento.
No se ha presentado en los últimos 5 años.	1	Rara vez	El evento puede ocurrir sólo en circunstancias excepcionales (poco comunes o anormales)

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

Tabla 3. **Impacto o consecuencias**

Descriptor	Descripción (Consecuencias) Cualitativo
Catastrófico	- Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

Mayor	- Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
Moderado	- Interrupción de las operaciones de la entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
Menor	- Interrupción de las operaciones de la entidad por algunas horas. - Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
Insignificante	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

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

8.1. Criterios Para Calificar El Impacto De Los Riesgos De Corrupción.

La Unidad acogió los criterios señalados por el DAFP, así:

Tabla 4. Criterios Para Calificar El Impacto De Los Riesgos De Corrupción

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		**10**	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

Nivel de impacto MAYOR

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

8.2. Criterios para Calificar los Riesgos de Seguridad Digital.

La exposición de un activo de información a una amenaza configura lo que se denomina un escenario de riesgo, el cual es evaluado a través de dos variables, la probabilidad de ocurrencia y el impacto que puede llegar a generar en la confidencialidad, integridad y disponibilidad de la información. Ambas variables permiten establecer el riesgo inherente cuya representación cuantitativa se construye a partir de la estimación de la vulnerabilidad, cuyo resultado se somete a los criterios de aceptabilidad de los riesgos de seguridad digital en la entidad.

8.3.1 Probabilidad

Estimar los criterios de probabilidad o frecuencia de ocurrencia del evento. Para este paso es necesario tener claro cada cuanto se presenta el escenario en donde se puede llegar a materializar el riesgo, de esta manera se pueden establecer adecuadamente las escalas descritas a continuación:

Tabla 5. Criterios para la valoración de la probabilidad de ocurrencia de los riesgos asociados al activo de Información

Valoración	Valor Asignado	Criterio
Raro	1	Evento que puede ocurrir solo en circunstancias excepcionales.
Improbable	2	El evento difícilmente puede ocurrir en algún momento.
Posible	3	El evento podría ocurrir en algún momento.
Probable	4	Es viable que el evento ocurra en la mayoría de las circunstancias.
Muy probable	5	Se espera que el evento ocurra en la mayoría de las circunstancias.

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

8.3.2 Impacto

Se adelantará la valoración del impacto generado, identificando los siguientes tres riesgos de seguridad digital (pérdida de la confidencialidad, pérdida de la integridad y pérdida de la disponibilidad); teniendo en cuenta los siguientes parámetros de evaluación:

Tabla No.6: Parámetros para la valoración del impacto de los riesgos asociados al activo de Información

Valoración	Valor Asignado	Criterio
Insignificante	1	Sin afectación a la confidencialidad, integridad y disponibilidad de la información.
Menor	2	Afectación leve de la confidencialidad, integridad y disponibilidad de la información.
Moderado	3	Afectación moderada de la confidencialidad, integridad y disponibilidad de la información.
Mayor	4	Afectación grave de la confidencialidad, integridad y disponibilidad de la información.
Catastrófico	5	Afectación muy grave de la confidencialidad, integridad y disponibilidad de la información.

Fuente: UPME

9. TRATAMIENTO DE RIESGOS

Es la respuesta que define la primera línea de defensa de la Entidad para mitigar los riesgos. Las opciones del tratamiento del riesgo incluyen aceptar, reducir, evitar o compartir los riesgos según se describe a continuación:

Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado).

Reducir el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos. Por lo general conlleva a la implementación de controles.

Evitar el Riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

Transferir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

10. PERIODICIDAD PARA EL SEGUIMIENTO DE ACUERDO CON EL NIVEL DE RIESGO RESIDUAL

10.1 Riesgos de Gestión y Corrupción

- Se realizarán actividades de seguimiento cuatrimestral por parte de los responsables de proceso para determinar la efectividad de los controles asociados a los riesgos y sobre las acciones de tratamiento sobre el riesgo residual. El GIT de Planeación brindará el apoyo requerido en su rol de segunda línea de defensa.
- El reporte del seguimiento se realizará de acuerdo con los lineamientos que defina el GIT de Planeación.
- Los responsables de proceso deben informar al GIT Planeación, cuando ocurran cambios del entorno o del proceso que puedan generar ajustes en cualquiera de las etapas de la administración del riesgo.
- El GIT de Planeación, consolida la gestión del riesgo e informa a la alta dirección sobre su estado.
- La Asesora de Control Interno realiza la evaluación independiente de la administración del riesgo - mapas de riesgos de corrupción de manera cuatrimestralmente de acuerdo con los términos legales y a los riesgos de gestión de acuerdo con las auditorías que adelante.
- Los mapas de riesgo se deben establecer o actualizar para cada vigencia, teniendo en cuenta que cada vigencia puede tener contextos diferentes. Igualmente, se podrán actualizar riesgos específicos en caso de requerirse por solicitud de los responsables de procesos o por temas que así lo ameriten.

10.2. Riesgos de Seguridad Digital

- El reporte del seguimiento se realizará de acuerdo con los lineamientos que defina la OGI
- Los responsables de proceso deben informar a la OGI, cuando ocurran cambios del entorno o del proceso que puedan generar ajustes en cualquiera de las etapas de la administración del riesgo.
- La Asesora de Control Interno realiza la evaluación independiente de la administración del riesgo - mapas de riesgos de seguridad digital de acuerdo con los términos legales en las auditorías que adelante.

CONTROL DE CAMBIOS

FECHA	VERSIÓN	MOTIVO DE CAMBIO
30 de abril de 2020	1	Creación del documento e inclusión en el Sistema de Gestión de Calidad
30 de junio de 2021	2	Se incluyó Objetivos específicos, matriz de responsabilidades de líneas de defensa y se realizó revisión y ajuste general del documento
13 de julio de 2031	3	Se realizó revisión general de acuerdo con la Guía del DAFP
01 de septiembre de 2021	4	Se incluye en la Política Integral el componente de Seguridad Digital