2025

Plan de tratamiento de riesgos de seguridad de la información

VERSIÓN EN REVISIÓN
FECHA 16/01/2025

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

APROBACIONES

Tabla 1

Aprobaciones

ELABORÓ		REVISÓ		APROBÓ	
Cargo:	Encargado seguridad de la información	Cargo:	Profesional Especializado	Cargo:	
Dependencia:	GRUPO TICS	Dependencia:	Grupo TICS	Dependencia:	OPGI
Fecha:	29/11/2024	Fecha:		Fecha:	

Fuente: MINENERGÍA

INDICE DE CONTENIDO

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

La gestión de riesgos en seguridad y privacidad de la información es fundamental para garantizar la protección de los activos críticos del Ministerio de Minas y Energía. En un entorno digital cada vez más dinámico, caracterizado por la adopción acelerada de nuevas tecnologías, el aumento de las amenazas cibernéticas y la evolución constante de la normativa, este plan busca fortalecer las capacidades institucionales para identificar, analizar y mitigar riesgos de manera eficiente y efectiva.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025 está diseñado como una herramienta estratégica que guía la implementación de controles específicos, alineados con estándares internacionales como la ISO/IEC 27001:2022, la ISO/IEC 31000:2018 y el NIST Cybersecurity Framework 2.0 (2024). Además, cumple con las directrices del Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el Gobierno de Colombia, asegurando el cumplimiento de las normativas nacionales e internacionales aplicables al sector.

Este documento se fundamenta en las lecciones aprendidas durante la vigencia del plan 2024, integrando mejoras basadas en auditorías, incidentes gestionados y evaluaciones internas. Incluye un enfoque renovado hacia la resiliencia organizacional, enfatizando no solo la respuesta efectiva ante eventos adversos, sino también la capacidad de prevenir y recuperarse de ellos, con un enfoque en la continuidad del negocio y la protección de la información estratégica del Ministerio.

El plan adopta una perspectiva integral que incluye tanto la seguridad técnica como la gestión organizacional. Esto abarca la implementación de medidas para proteger la confidencialidad, integridad y disponibilidad de la información, así como la educación y capacitación continua de los colaboradores, promoviendo una cultura organizacional que valore la seguridad como un pilar esencial para alcanzar los objetivos estratégicos.

Por último, este plan no solo establece un marco claro para gestionar riesgos, sino que también refuerza el compromiso del Ministerio con la mejora continua. A través de un monitoreo y evaluación constante, se garantiza que las medidas implementadas sean efectivas y adaptables a las necesidades cambiantes del sector energético y minero. Esto permite que el Ministerio de Minas y Energía continúe liderando con confianza en un entorno de amenazas emergentes y demandas normativas.

2. JUSTIFICACIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025 responde a la necesidad de mitigar los riesgos asociados con la gestión de datos sensibles y las operaciones críticas del Ministerio de Minas y Energía. En un contexto donde las amenazas cibernéticas son cada vez más sofisticadas, este plan proporciona una hoja de ruta estratégica para implementar controles específicos que garanticen la confidencialidad, integridad y disponibilidad de la información. Además, fortalece la resiliencia de la entidad frente a posibles interrupciones operativas, asegurando la continuidad de sus servicios esenciales.

La incorporación de estándares internacionales como la ISO/IEC 27001:2022, la ISO/IEC 31000:2018 y el NIST Cybersecurity Framework 2.0 (2024), junto con la normativa nacional, permite al Ministerio alinear su gestión de riesgos con las mejores prácticas globales. Este enfoque integral no solo atiende las vulnerabilidades identificadas en evaluaciones previas, sino que también prepara a la organización para enfrentar amenazas emergentes, adaptando continuamente sus estrategias a un panorama de riesgos dinámico. El plan, por tanto, no se limita a la implementación de medidas correctivas, sino que promueve una cultura organizacional de seguridad, donde todos los colaboradores comprenden su rol en la protección de la información.

3. CONTEXTUALIZACIÓN

El MINENERGÍA cuenta con un repositorio para el Sistema de Gestión de Calidad, donde las diferentes dependencias publican sus riesgos, la actualización de estos riesgos se realiza cada año según las directrices de la Oficina de Planeación y Gestión Internacional del MINENERGÍA. A excepción de algunos riesgos publicados por el Grupo de Tecnología de la Información y las Comunicaciones TICS, sobre la gestión de la información, no se evidencian riesgos de información postulados por otras dependencias, aunque de manera intrínseca está si los tengan dentro de sus procesos temáticos y funcionales.

4. ANTECEDENTES

La evolución de los riesgos asociados a la seguridad y privacidad de la información ha llevado al Ministerio de Minas y Energía a implementar estrategias integrales y estructuradas para gestionar estas amenazas de manera efectiva. Desde la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI), el Ministerio ha fortalecido sus capacidades institucionales mediante la incorporación de normativas como la ISO/IEC 27001, ajustándose a los cambios normativos nacionales, incluyendo la reciente Resolución 40646 de 2023, que establece lineamientos específicos para proteger los sistemas de información de la entidad.

Durante el año 2024, el Ministerio desarrolló un marco robusto de gestión de riesgos, que facilitó el registro y control de actividades críticas como la identificación de activos (matriz desarrollada), la evaluación de riesgos en desarrollo y el manejo de incidentes (procedimientos). Estas acciones permitieron una mayor visibilidad sobre las vulnerabilidades de la entidad, impulsando la implementación de controles correctivos y la priorización de activos críticos (procesos actuales).

Además, las auditorías internas y externas realizadas evidenciaron la necesidad de ajustes en los procedimientos para responder con mayor agilidad a las amenazas emergentes.

A medida que el panorama de ciberseguridad continúa evolucionando, el Ministerio ha identificado la importancia de alinear sus estrategias con estándares internacionales y mejores prácticas globales. El enfoque adoptado para el 2025 no solo integra las lecciones aprendidas de ejercicios anteriores, sino que también responde a desafíos como la protección de infraestructuras críticas del sector energético, la gestión de riesgos asociados con tecnologías emergentes, y el fortalecimiento de la cultura organizacional en seguridad de la información.

5. OBJETIVOS

A continuación, se presentan el objetivo general y los objetivos específicos:

5.1 OBJETIVO GENERAL

Generar un plan para el tratamiento de los riesgos de seguridad estudiados en la Entidad, de tal forma que el cálculo de riesgo inherente se pueda llevar a un valor que se encuentre por debajo del nivel de aceptación aprobado en el MINENERGIA.

5.2 OBJETIVOS ESPECÍFICOS

A) Establecer actividades para la mitigación de riesgos.
B) Generar una hoja de ruta en donde se estipulen responsables y duración para la implementación de las actividades de mitigación de riesgos.

6. ALCANCE

El tratamiento de riesgos prioriza aquellos clasificados como altos o críticos, estableciendo controles específicos para mitigar las amenazas identificadas. La hoja de ruta asociada incluye la asignación de responsables, tiempos de implementación y mecanismos de evaluación para garantizar que los controles implementados sean efectivos. Además, se destacan acciones como la implementación de prácticas de desarrollo seguro, el uso de herramientas criptográficas avanzadas, y la capacitación continua del personal en clasificación y protección de información.

Este enfoque integral no solo permite abordar vulnerabilidades específicas, sino que también fortalece la postura de seguridad general del Ministerio. Al priorizar las actividades de mitigación y monitorear su impacto, la matriz de riesgos asegura una mejora continua en la resiliencia operativa , preparándolo para enfrentar amenazas emergentes y desafíos tecnológicos en un entorno digital dinámico.

7. PLAN DE TRATAMIENTO DE RIESGOS

A continuación, se describe el Plan de Tratamiento de Riesgos analizados con base en la matriz de riesgos de Grupo TICS:

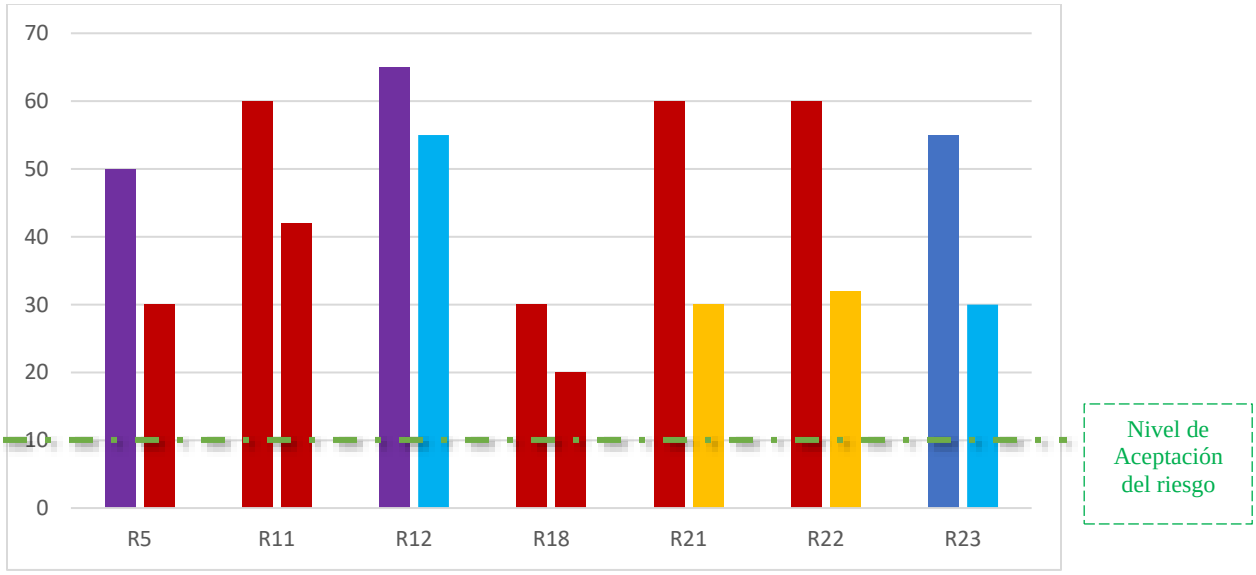
7.1 VALORACIÓN RIESGO RESIDUAL

la valoración del riesgo residual es una etapa clave para determinar la eficacia de los controles implementados y garantizar que los riesgos se mantengan dentro de niveles tolerables para el Ministerio de Minas y Energía. Este proceso en las directrices de la *Guía para la Administración del Riesgo (Versión 6) del DAFP*.

La valoración del riesgo residual para 2025 incorporará un análisis más granular de los controles existentes, midiendo no solo su implementación, sino también su efectividad en reducir los riesgos inherentes. Este análisis incluirá métricas claras, como el porcentaje de reducción del riesgo tras la implementación de los controles, y priorizará aquellos riesgos con mayor impacto sobre los sistemas críticos, como plataformas tecnológicas, bases de datos estratégicas y servicios en la nube.

El objetivo para 2025 es garantizar que los riesgos residuales se mantengan dentro de los límites establecidos por la entidad, priorizando una mejora continua. Las vulnerabilidades con niveles residuales inaceptables serán objeto de nuevos tratamientos, incluyendo la implementación de controles adicionales o la revisión de los procesos existentes. Este enfoque adaptativo refuerza el compromiso del Ministerio con la seguridad de la información y la protección de sus activos estratégicos frente a amenazas dinámicas y emergentes.

Ilustración 1 - Comparativo Riesgo Residual e Inherente por número de riesgo.



Fuente: Grupo TICS

7.2 VULNERABILIDADES A ELIMINAR DE LOS RIESGOS QUE REQUERIEN TRATAMIENTO

Para 2025, se identifican y priorizan aquellas vulnerabilidades críticas que deben ser eliminadas o tratadas de manera inmediata para reducir los riesgos residuales a niveles aceptables. Entre estas se incluyen la falta de prácticas de desarrollo seguro, la ausencia de monitoreo efectivo de registros (logs), y debilidades en los controles criptográficos. Estas vulnerabilidades representan un impacto significativo en la seguridad de los activos tecnológicos y requieren la implementación de controles técnicos y organizacionales específicos para mitigar los riesgos asociados.

El enfoque para el tratamiento de estas vulnerabilidades en 2025 está orientado a fortalecer las capacidades técnicas mediante herramientas avanzadas de monitoreo, establecer procedimientos claros para la recuperación ante incidentes, y garantizar la disposición segura de dispositivos que contienen información sensible. Además, se promoverá una estrategia de capacitación específica para los equipos involucrados, complementada con revisiones trimestrales para evaluar la efectividad de los controles implementados y realizar los ajustes necesarios. Este enfoque refuerza el compromiso del Ministerio con la protección integral de sus activos críticos y la mejora continua de su postura de seguridad.

Tabla 3

Vulnerabilidades para mitigar 2025

No. Riesgo	NOMBRE DEL RIESGO
R5	Software – Seguimiento estricto de prácticas de desarrollo seguro. Aunque ya existe la metodología hay que establecer protocolos y cumplimiento de requerimientos para los SI.
R11	Falta de monitoreo a Logs de seguridad y registro, además de esto son eliminados sin control alguno.
R12	Personas - Los funcionarios del Ministerio no firman acuerdos de confidencialidad. No se evidencian cláusulas de confidencialidad aplicadas a los funcionarios, contratistas y proveedores.
R18	No se tiene un estándar para el manejo de información confidencial. No se utilizan herramientas tecnológicas para controles criptográficos.
R21	Falencias en la clasificación de información – sin actualización desde 2021 No se tiene por ende BIA y BCP actualizados.
R22	Ausencia de mecanismos de renovación oportuna de contratos
R23	Procedimiento Gestión de Continuidad y Recuperación de los Servicios de Informática y Comunicaciones. Ausencia de DRP actualizado.

Fuente: Grupo TICS

Las actividades que se deben ejecutar para mitigar todas estas vulnerabilidades se pueden observar directamente en el documento “Plan de tratamiento de riesgos.xls” en donde adicionalmente se puede ver la duración de cada actividad y el responsable de su ejecución.

De igual forma se puede encontrar la hoja de ruta de este plan de tratamiento donde en la parte superior se pueden observar los meses (M1, M2, …M12) y sus semanas (S1, S2, S3 y S4), el código de riesgo en la primera columna (R1, R2, Rn), y su cruce con el número de la actividad relacionada con ese riesgo, tal como se puede observar en la Ilustración 2.

Ilustración 2 *– Hoja de ruta plan de tratamiento de riesgos.*

Energía

FORMATO

PLAN DE TRATAMIENTO DE RIESGOS

SIG Sistema Integrado de Gestión del Minenergía

	M1				M2				M3				M4				M5				M6				M7				M8				M9				M10			
	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
R5					1	1	1	1	2	2	2	2													3	3	4	4	5	5	5	5								
R11									1	1	1	1									2	2	2	2					3	3	3	3								
R12									1	1	1	1									2	2	2	2					3	3	3	3								
R18	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4	4	5	5	5	5
R21	1	1	1	1	2	2	2	2	3	3	3	3																												
R22									1	1	1	1									2	2	2	2					3	3	3	3								
R23									1	1	1	1	2	2	2	2	3	3	3	3																				

Fuente: Grupo TICS

8. RECOMENDACIONES

fortalecer la gestión de riesgos de seguridad y privacidad de la información, asegurando que los controles implementados sean efectivos y alineados con las mejores prácticas y estándares internacionales. Estas recomendaciones surgen del análisis de vulnerabilidades críticas, resultados de auditorías y el contexto normativo vigente.

1. **Priorizar el tratamiento de riesgos altos**: Los riesgos clasificados como críticos deben ser atendidos de forma prioritaria, implementando medidas correctivas que reduzcan su probabilidad e impacto. Esto incluye reforzar controles criptográficos, mejorar prácticas de desarrollo seguro y garantizar la disposición segura de dispositivos que contienen información sensible.
2. **Evaluación periódica de controles**: Se recomienda realizar al menos una evaluación anual de los controles implementados, verificando si han logrado mitigar efectivamente los riesgos y ajustando las estrategias según los resultados obtenidos.
3. **Alineación con guías y normativas**: El plan debe mantenerse actualizado con las recomendaciones del Departamento Administrativo de la Función Pública (DAFP) y estándares como la ISO/IEC 27001:2022, integrando mejoras sugeridas por las auditorías internas y externas.

Estas recomendaciones son esenciales para garantizar la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) y para fortalecer la resiliencia del Ministerio frente a amenazas emergente.

9. GLOSARIO

DAFP: Departamento Administrativo de la Función Pública

10. REFERENCIAS

DAFP. (2020). *Guía para la administración del riesgo y el diseño de controles en entidades púiblicas versión 5.* Bogotá: DAFP.