

2025

Plan de seguridad y privacidad de la información

PLAN DE SEGURIDAD Y PRIVACIDAD 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

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INDICE DE CONTENIDO

APROBACIONES	2
1. INTRODUCCIÓN.....	5
2. JUSTIFICACIÓN	6
3. CONTEXTUALIZACIÓN	7
4. ANTECEDENTES	7
5. OBJETIVOS	8
5.1 OBJETIVO GENERAL	9
5.2 OBJETIVOS ESPECÍFICOS	9
6. ALCANCE	9
7. PLAN DE SEGURIDAD DE LA INFORMACIÓN	10
7.1 PLAN OPERACIONAL DE SEGURIDAD DE LA INFORMACIÓN	10
7.1.1 GESTIÓN DE ACTIVOS DE INFORMACIÓN	10
7.1.2 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.....	11
7.1.3 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	13
7.1.4 GESTIÓN DE POLÍTICAS Y PROCEDIMIENTOS	13
7.1.5 GESTIÓN DE RECURSOS DE SEGURIDAD	14
7.2 PLAN DE ASEGURAMIENTO Y EVALUACIÓN DE LA IMPLEMENTACIÓN Y MANTENIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN	15
7.2.1 GESTIÓN DE INDICADORES	15
7.2.2 GESTIÓN DE VULNERABILIDADES	18
7.2.3 PLAN DE AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN.....	20
7.2.4 PLAN DE MEJORAMIENTO CONTINUO.....	22
7.2.5 REVISIÓN POR LA ALTA DIRECCIÓN.....	23
7.3 PLAN DE COMUNICACIONES	24
7.3.1 CARACTERIZACIÓN DE INTERESADOS	24
7.3.2 COMUNICACIONES	26
7.4 PLAN DE SENSIBILIZACIÓN Y CAPACITACIÓN.....	27
7.4.1 SENSIBILIZACIÓN	28
7.4.1.1 MODALIDAD	29
7.4.1.2 MEDIOS.....	29
7.4.2 CAPACITACIÓN.....	30
7.4.2.1 DEFINICIÓN DE PÚBLICOS OBJETIVO.....	30
7.4.2.3 MEDIOS	31
7.4.2.1 SELECCIÓN DE TEMAS	34
8. RECOMENDACIONES.....	36

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

9.	MEJORES PRÁCTICAS.....	37
10.	GLOSARIO.....	38
11.	REFERENCIAS	40

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

La capacidad de acceder a la información a través de Internet desde múltiples dispositivos electrónicos, el incremento de los servicios digitales y el auge creciente de las nuevas tecnologías han dado un impulso significativo a la digitalización en los últimos años. La pandemia de COVID-19, por su parte, catalizó una transformación sin precedentes, obligando a las entidades públicas en Colombia a adoptar medios digitales y modalidades de interacción remota para garantizar la continuidad de sus servicios. Esta transición acelerada consolidó el uso de ambientes colaborativos, recuperación de datos remotos y dispositivos electrónicos en las operaciones diarias, pero también incrementó la exposición a ciberataques y a vulnerabilidades en los sistemas de información.

El Ministerio de Minas y Energía, alineado con su compromiso institucional, ha trabajado constantemente en la creación de entornos seguros que permitan salvaguardar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional. Durante el 2024, se evidenció que la creciente dependencia de los datos digitales incrementó su valor estratégico, al tiempo que elevó el riesgo de incidentes cibernéticos. A pesar de las medidas adoptadas, el sector público enfrentó eventos significativos, como la explotación de vulnerabilidades en proveedores de servicios en la nube, afectando a diversas entidades gubernamentales.

El Plan de Seguridad y Privacidad de la Información 2025 es el resultado de analizar, implementar y adaptar lecciones aprendidas de periodos anteriores, incorporando las mejores prácticas internacionales y normativas nacionales. Este documento tiene como propósito fundamental garantizar la resiliencia de los sistemas de información del Ministerio, fortaleciendo la protección de los activos digitales y alineándose con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, así como con estándares reconocidos como la ISO/IEC 27001:2022, la ISO/IEC 22301:2019, y la ISO/IEC 31000:2018.

A lo largo del 2024, el Grupo de Tecnologías de la Información y las Comunicaciones (TICs) del Ministerio consolidó avances importantes en la gestión de riesgos, la protección de datos y la promoción de una cultura de seguridad en todos los niveles de la organización. Las políticas, procedimientos y protocolos actualizados han permitido un cumplimiento más efectivo de las exigencias del MSPI y de las directrices internacionales. Este plan 2025 busca no solo consolidar estas acciones, sino también anticiparse a las tendencias emergentes en ciberseguridad, fomentando un enfoque adaptativo y proactivo frente a las amenazas.

En el marco del Plan 2025, se busca fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI) del Ministerio, integrando controles administrativos, técnicos y operativos que garanticen la protección de la información. Además, este plan refuerza el compromiso del Ministerio con la implementación del ciclo PHVA (Planificar, Hacer, Verificar y Actuar), fomentando la mejora continua en los procesos de seguridad de la información.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El enfoque también incluye la gestión de incidentes mediante un esquema estructurado basado en los pilares del NIST Cybersecurity Framework: Identificar, Proteger, Detectar, Responder y Recuperar. Este marco permitirá fortalecer la resiliencia organizacional y garantizar la continuidad operativa, incluso frente a escenarios complejos de ciberamenazas.

El presente plan tiene como objetivo central proteger la información institucional, salvaguardar los derechos de las partes interesadas y asegurar el cumplimiento normativo nacional e internacional. Este propósito se logrará mediante acciones como:

- La promoción de una cultura organizacional de seguridad de la información.
- La implementación de controles específicos para mitigar riesgos.
- El diseño de estrategias de capacitación y sensibilización dirigidas a todos los niveles del Ministerio.

El Ministerio de Minas y Energía reafirma su compromiso con la protección de los datos y la información como un activo estratégico. A través del Plan 2025, se busca consolidar un entorno digital seguro, resiliente y transparente, que no solo permita una gestión eficiente de los recursos, sino que también contribuya a fortalecer la confianza ciudadana. Este plan será revisado periódicamente para adaptarse a los retos tecnológicos y normativos emergentes, asegurando su vigencia y relevancia.

2. JUSTIFICACIÓN

La seguridad de la información es un pilar estratégico para cualquier organización en la era digital, especialmente en entidades gubernamentales encargadas de regular sectores tan sensibles como el energético y minero. En este contexto, el cumplimiento del ciclo PHVA (Planificar, Hacer, Verificar y Actuar) se convierte en una herramienta fundamental para la mejora continua de los sistemas de gestión de seguridad de la información. Este enfoque permite abordar las crecientes amenazas cibernéticas con acciones preventivas, correctivas y adaptativas, asegurando así la protección de los activos críticos del Ministerio de Minas y Energía.

El cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC exige la implementación de controles específicos que garanticen los cuatro pilares fundamentales de la seguridad de la información: confidencialidad, para evitar accesos no autorizados; integridad, para asegurar la exactitud y completitud de los datos; disponibilidad, para garantizar el acceso oportuno a la información; y privacidad, para proteger los datos personales y sensibles frente a su uso indebido. Estos principios no solo respaldan las operaciones del Ministerio, sino que también fortalecen la confianza de los ciudadanos en la gestión pública.

Además, en un entorno global donde las ciberamenazas evolucionan constantemente, resulta indispensable contar con un plan estratégico que permita identificar, evaluar y mitigar riesgos de

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

manera efectiva. El Plan de Seguridad y Privacidad de la Información 2025 responde a esta necesidad, proporcionando un marco para la gestión estructurada de los riesgos asociados a la información institucional. Este documento también facilita el seguimiento de las actividades anuales, permitiendo a la entidad ajustar sus estrategias según las lecciones aprendidas y las nuevas normativas, como lo establece la Resolución 40646 de 2023.

Finalmente, el plan justifica su importancia al promover una cultura de seguridad organizacional que trasciende las medidas técnicas y fomenta el compromiso de todos los niveles del Ministerio. La sensibilización y capacitación continua del personal, junto con la implementación de auditorías periódicas y la evaluación de indicadores clave, garantizan que el Ministerio pueda cumplir con su misión de manera eficiente y resiliente. Este enfoque no solo protege la información institucional, sino que también refuerza la credibilidad y la transparencia en la gestión pública, elementos esenciales para el fortalecimiento de las políticas gubernamentales y la confianza ciudadana.

3. CONTEXTUALIZACIÓN

El Ministerio de Minas y Energía, como entidad rectora del sector energético y minero en Colombia, enfrenta un entorno digital cada vez más complejo y dinámico. En los últimos años, el auge de las tecnologías de la información, el incremento de los servicios en la nube, y la creciente dependencia tecnológica han transformado los procesos internos, exigiendo una gestión más robusta de la seguridad y privacidad de la información. Este plan responde a la necesidad de proteger los activos críticos de la entidad frente a riesgos cibernéticos y garantizar la continuidad operativa en un contexto normativo y tecnológico en constante evolución.

Durante la vigencia 2024, el Ministerio implementó diversas estrategias alineadas con el Modelo de Seguridad y Privacidad de la Información (MSPI), integrando herramientas tecnológicas y adoptando estándares internacionales como la ISO/IEC 27001:2022 y la ISO/IEC 31000:2018. Sin embargo, persisten desafíos asociados con la rápida evolución de las amenazas cibernéticas, el cumplimiento normativo y la capacitación continua de los colaboradores, aspectos que este plan busca abordar de manera integral.

El Plan de Seguridad y Privacidad de la Información 2025 consolida un enfoque basado en la mejora continua, apoyado en el ciclo PHVA (Planificar, Hacer, Verificar, Actuar). Este enfoque prioriza la identificación de riesgos, la implementación de controles efectivos y la promoción de una cultura organizacional de seguridad. Así, el Ministerio se prepara para enfrentar los retos del entorno digital, protegiendo sus activos de información, fortaleciendo su resiliencia operativa, y contribuyendo a su misión estratégica en el sector minero-energético de Colombia.

4. ANTECEDENTES

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Ministerio de Minas y Energía ha venido fortaleciendo de manera progresiva su capacidad para gestionar la seguridad y privacidad de la información, en línea con los requerimientos establecidos en la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC. Durante los últimos años, la entidad ha centrado sus esfuerzos en el cumplimiento de las normativas nacionales, optimizando sus procesos de diagnóstico, planeación estratégica y actualización de políticas para abordar de manera eficiente los riesgos asociados a la gestión de datos en un entorno cada vez más digitalizado.

En 2024, el Ministerio consolidó avances importantes en la implementación de la Resolución 40646 de 2023, la cual formalizó las políticas específicas aplicables al MSPI. Estas políticas proporcionaron una guía para la gestión integral de riesgos, la protección de la información sensible y la mejora de la resiliencia ante incidentes cibernéticos. Durante este período, el Grupo de Tecnologías de la Información y las Comunicaciones (TICs) lideró iniciativas orientadas a reforzar los cuatro pilares fundamentales de la seguridad de la información: confidencialidad, integridad, disponibilidad y privacidad. Estas acciones permitieron fortalecer los controles existentes, garantizar la protección de los activos digitales y fomentar una cultura organizacional alineada con los principios de seguridad.

No obstante, 2024 también evidenció retos importantes, como el incremento en la sofisticación de las ciberamenazas que impactaron sectores estratégicos, incluida la afectación a entidades públicas a través de vulnerabilidades en servicios de nube. Estos eventos destacaron la necesidad de adoptar un enfoque más amplio y adaptativo en la gestión de riesgos. Aunque el Ministerio avanzó en la implementación de medidas correctivas y preventivas, no se utilizó ningún marco normativo internacional como el NIST Cybersecurity Framework, cuya integración está proyectada para el 2025. Esto marca un nuevo enfoque para alinear las prácticas del Ministerio con estándares internacionales y mejorar la gestión integral de la seguridad digital.

El Plan de Seguridad y Privacidad de la Información 2025 refleja este aprendizaje acumulado, incorporando los lineamientos del NIST CSF, junto con los ya establecidos en normativas como la ISO/IEC 27001:2022 y guías del MSPI. Este marco de trabajo permitirá al Ministerio no solo consolidar las acciones previas, sino también desarrollar nuevas estrategias para anticiparse a los riesgos emergentes, mejorar la capacidad de respuesta ante incidentes y garantizar la continuidad operativa en un entorno altamente dinámico y complejo.

5. OBJETIVOS

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

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.1 OBJETIVO GENERAL

Establecer las directrices para la gestión y seguimiento de la seguridad de la información por medio de actividades de control y planes de acción que ayuden a mantener la confidencialidad, integridad, disponibilidad y privacidad de la información, así como la relación de los procedimientos asociados a las políticas establecidas que permitan asegurar la protección y persistencia de la SI.

5.2 OBJETIVOS ESPECÍFICOS

- a) Contribuir al incremento de la transparencia, frente a la gestión pública.
- b) Dar lineamiento para la implementación de la gestión de la seguridad y privacidad de la información.
- c) Establecer las actividades anuales a ejecutar en temas de Seguridad de la Información.
- d) Concentrar los planes relacionados con Seguridad de la Información en un punto único de consulta y gestión.

6. ALCANCE

El Plan de Seguridad y Privacidad de la Información 2025 del Ministerio de Minas y Energía abarca todos los procesos, activos, personas y sistemas que intervienen en la gestión, uso y protección de la información institucional. Este alcance se extiende a las dependencias internas del Ministerio, sus colaboradores, contratistas y terceros que gestionen datos o recursos relacionados con sus operaciones, con el fin de garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información.

En términos de infraestructura tecnológica, el plan cubre la totalidad de los sistemas de información, redes de comunicación, bases de datos, aplicaciones y equipos de cómputo utilizados por el Ministerio. Esto incluye tanto los entornos físicos como los virtuales y en la nube, con especial énfasis en la protección de activos críticos relacionados con la regulación y supervisión del sector energético y minero. También considera la implementación y mantenimiento de controles de seguridad aplicables a los procesos misionales, administrativos y estratégicos, asegurando que cumplan con las normativas nacionales e internacionales vigentes.

Adicionalmente, el alcance incluye la interacción con partes externas, como proveedores de servicios tecnológicos, organismos reguladores y ciudadanos que acceden a los servicios del Ministerio. Se enfatiza la necesidad de establecer acuerdos de nivel de servicio (SLAs) y protocolos de gestión de riesgos para garantizar que los terceros cumplan con las políticas de seguridad definidas. Este enfoque integral asegura que todos los aspectos relacionados con la seguridad de la información sean tratados de manera coherente y robusta, contribuyendo a la resiliencia organizacional y a la confianza de los grupos de interés.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

7. PLAN DE SEGURIDAD DE LA INFORMACIÓN

7.1 PLAN OPERACIONAL DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se describen los componentes que hace parte del plan operativo de seguridad de la Información:

7.1.1 GESTIÓN DE ACTIVOS DE INFORMACIÓN

El Plan de Seguridad y Privacidad de la Información 2025 establece que la gestión de activos de información debe ser un proceso continuo que incluya la identificación, clasificación, actualización y protección de los activos tecnológicos, físicos y de información. Esto garantiza que los activos relevantes para el cumplimiento de los objetivos del Ministerio estén debidamente gestionados y protegidos frente a amenazas y materialización de riesgos.

En diciembre de 2025, se dará inicio a la capacitación de los responsables en el uso de la nueva matriz de activos, enfocada en asegurar que estos sean capaces de identificar y clasificar los activos bajo su gestión, custodio y sobre todo enfocarse en establecer los procesos correspondientes que permita al ministerio la debida gestión y estrategia de seguridad de la información que permita la construcción de los análisis de impacto al negocio (BIA) y los planes de continuidad del negocio (BCP) para el establecimiento del Plan de recuperación ante desastres (DRP) y donde sea necesario usar dichos procesos.

Tabla 3.

Actualización cronograma de actividades- Matriz de activos de información

Actividad	Responsable	Fecha de Inicio	Fecha de Finalización	Descripción
Capacitación sobre la matriz de activos	Oficial de Seguridad o quien haga sus veces	Primera semana - Febrero 2025	Segunda semana - Febrero 2025	Capacitar a los responsables en el uso de la matriz y en los principios básicos de activos de información.
Llenado inicial de la matriz de activos	Responsables de cada dependencia	Segunda semana - Febrero 2025	Primera semana - Marzo 2025	Identificar y clasificar activos de información según los procesos de cada área
Revisión primaria de información enviada por las dependencias	Oficial de Seguridad o quien haga sus veces	Segunda semana - Marzo 2025	Tercera semana - Marzo 2025	Revisar documentación enviada por las dependencias (responsables), unificar información y establecer retroalimentación y mejora continua.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Ajustes y envío de retroalimentación a dependencias	Oficial de Seguridad o quien haga sus veces	Cuarta semana - Marzo 2025	Primera Semana - Abril 2025	En caso de presentarse información faltante o incompleta generar retroalimentación.
Entrega de información ajustada	Responsables de cada dependencia	Segunda Semana - Abril 2025	Cuarta semana - Abril 2025	Información debidamente ajustada y completada.
Validación y priorización de activos críticos	Oficial de Seguridad o quien haga sus veces	Cuarta semana - Abril 2025	Segunda semana - Mayo 2025	Revisar, validar y priorizar los activos críticos según el impacto al negocio y continuidad al mismo.
Integración con el SGSI	Oficina de planeación y gestión territorial	Segunda semana - Mayo 2025	Cuarta semana - Mayo 2025	Incorporar los activos priorizados en el SGSI y actualizar los controles.

Fuente grupo TICS

7.1.2 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de riesgos de seguridad de la información es un componente esencial del Plan de Seguridad y Privacidad de la Información 2025, ya que permite identificar, evaluar y mitigar las amenazas que podrían comprometer la confidencialidad, integridad, disponibilidad y privacidad de los activos críticos del Ministerio de Minas y Energía.

El Ministerio adoptará un enfoque sistemático para la gestión de riesgos, integrando los siguientes procesos clave:

1. **Identificación de riesgos:** Determinar las amenazas potenciales, las vulnerabilidades explotables y los activos en riesgo (Riesgos de gestión TICS)
2. **Evaluación de riesgos:** Aplicar metodologías para analizar la probabilidad de ocurrencia e impacto de cada riesgo identificado, priorizándolos según su criticidad.
3. **Tratamiento de riesgos:** Definir e implementar medidas de control específicas para mitigar, transferir, aceptar o evitar los riesgos, asegurando que estas acciones sean proporcionales al nivel de riesgo.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

4. **Monitoreo y revisión:** Establecer un sistema continuo de monitoreo para identificar cambios en el entorno que puedan alterar el perfil de riesgo del Ministerio, incluyendo revisiones trimestrales y auditorías anuales.
5. **Documentación y comunicación:** Garantizar que todos los procesos de gestión de riesgos estén debidamente documentados y que los resultados sean comunicados a las partes interesadas.

Tabla 4.

Hoja de ruta gestión de riesgos de seguridad de la información.

Actividad	Responsable	Fecha de Inicio	Fecha de Finalización	Descripción
Ajustes plan de tratamiento de riesgos de seguridad de la información	Oficial de Seguridad o quien haga sus veces	Primera semana - Febrero 2025	Tercera semana - Febrero 2025	A partir de la recomendaciones u hallazgos, ajustar actividades y procesos del plan de tratamiento de riesgos.
Aprobación de análisis de riesgos	Oficina de planeación y gestión territorial (OPGI)	Tercera semana - Febrero 2025	Cuarta semana - Febrero 2025	Aprobación del plan de tratamiento de riesgos de seguridad de la información.
Evaluación de riesgos	Oficial de Seguridad o quien haga sus veces	Primera semana - Marzo 2025	Tercera semana - Marzo 2025	Análisis de impacto y probabilidad para priorizar riesgos en todas las áreas.
Desarrollo del plan de tratamiento	Oficial de Seguridad o quien haga sus veces	Primera semana - Abril 2025	Seguimiento trimestral	Diseñar controles y medidas correctivas para mitigar riesgos identificados, seguimiento del plan y avance en la disminución de la probabilidad de materialización del riesgo.
Implementación de controles	Oficial de Seguridad o quien haga sus veces	Seguimiento trimestral	Seguimiento trimestral	Ejecutar las medidas aprobadas y documentarlas en el SGSI.
Auditoría de gestión de riesgos	Control Interno	Tercer trimestre año 2025	Tercer trimestre año 2025	Evaluar la eficacia de las medidas implementadas y preparar un informe final.

Fuente grupo TICS

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

7.1.3 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Atendiendo las indicaciones y recomendaciones de la Oficina de Planeación y Gestión Internacional, en el sentido que, para la presente vigencia este Plan, se adaptara y adoptara la misma metodología de trabajo dispuesta desde la “Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6”, expedida por el DAFP en noviembre de 2022, para lo cual los riesgos descritos tanto en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, como los riesgos de la gestión TIC, tendrán seguimiento y control trimestral durante la vigencia 2025

7.1.4 GESTIÓN DE POLÍTICAS Y PROCEDIMIENTOS

El Ministerio desarrollará, actualizará y gestionará sus políticas y procedimientos de seguridad de la información con base en las siguientes directrices:

1. **Estructura centralizada:** Consolidar todas las políticas y procedimientos relacionados con la seguridad de la información en un punto único de consulta, facilitando su acceso y uso por parte de todas las partes involucradas tanto internas como externas.
2. **Ciclo de vida de las políticas:** Establecer un ciclo de vida que incluya la creación, aprobación, difusión, implementación, monitoreo y actualización de las políticas. Cada política debe estar alineada con las normativas aplicables y revisarse al menos una vez al año.
3. **Capacitación continua:** Garantizar que los responsables y colaboradores comprendan las políticas mediante sesiones de formación, con especial atención a aquellas áreas que interactúan directamente con activos críticos.
4. **Monitoreo de cumplimiento:** Realizar auditorías regulares para evaluar la adherencia a las políticas y su efectividad en la mitigación de riesgos.
5. **Adaptabilidad y mejora continua:** Ajustar las políticas y procedimientos en respuesta a cambios regulatorios, tecnológicos y operativos, asegurando que sigan siendo pertinentes y efectivas.

Tabla 5.

Gestión de Políticas y Procedimientos de Seguridad de la Información

Actividad	Responsable	Fecha de Inicio	Fecha de Finalización	Descripción
Entrega de políticas y procedimientos de acuerdo a la resolución 40646 para la vigencia 2025	Oficial de Seguridad o quien haga sus veces	Primera semana febrero 2025	Primera semana febrero 2025	Entrega de procedimientos y políticas debidamente actualizadas, ajustadas o estructuradas para primera revisión por parte del grupo TICS.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Creación de nuevos procedimientos	Oficial de Seguridad o quien haga sus veces	Primera semana febrero 2025	- Tercera semana febrero 2025	Diseñar procedimientos específicos para áreas críticas no cubiertas actualmente.
Aprobación de políticas y procedimientos	Comité institucional de gestión y desempeño.	Cuarta semana Febrero 2025	- Primera semana Marzo 2025	Validar y aprobar las políticas y procedimientos actualizados o nuevos.
Capacitación de uso de procedimientos y conocimiento de políticas	Oficial de Seguridad o quien haga sus veces	Primera semana Marzo 2025	- Cuarta semana Junio 2025	Socializar los cambios y formar a los responsables en su implementación.
Monitoreo de cumplimiento	Oficial de Seguridad o quien haga sus veces	Seguimiento trimestral	Seguimiento trimestral	Auditorías internas para verificar la adherencia y la efectividad de las políticas.
Revisión anual	Oficial de Seguridad o quien haga sus veces	Primera semana Diciembre 2025	- Primera semana Diciembre 2025	Evaluar el estado general de las políticas y procedimientos para preparar el ciclo 2026.

Fuente grupo TICS

7.1.5 GESTIÓN DE RECURSOS DE SEGURIDAD

La gestión de recursos de seguridad del Plan de Seguridad y Privacidad de la Información 2025 tiene como objetivo asegurar que el Ministerio de Minas y Energía cuente con los recursos humanos, tecnológicos y financieros necesarios para implementar, mantener y mejorar continuamente su postura de seguridad de la información. Este enfoque garantiza que los controles establecidos para proteger la confidencialidad, integridad, disponibilidad y privacidad de la información estén respaldados por una asignación eficiente y estratégica de recursos.

El Ministerio prioriza la adquisición y mantenimiento de herramientas tecnológicas críticas para la detección y mitigación de riesgos, tales como sistemas de monitoreo continuo (SIEM), firewalls de próxima generación, plataformas de gestión de vulnerabilidades, y sistemas de respaldo y recuperación. Estas soluciones permiten proteger la infraestructura tecnológica en todos los niveles, incluyendo sistemas en la nube y redes internas. La asignación de recursos financieros está orientada a cubrir tanto las inversiones en tecnología como los procesos de auditoría y mejora continua.

Adicionalmente, la gestión de recursos busca optimizar el uso del presupuesto disponible para responder a cambios en el entorno regulatorio o amenazas emergentes. El enfoque del plan es dinámico, permitiendo evaluar periódicamente la efectividad de los recursos asignados y

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

priorizando inversiones en áreas críticas que impacten directamente los objetivos estratégicos del Ministerio, como la protección de los activos más sensibles

Las actividades por ejecutar para este análisis se pueden consultar en la **Tabla 2**.

Tabla 2

Gestión de Recursos de Seguridad

No	Descripción de la actividad	Responsable	Fecha
1	Establecer las necesidades de presupuesto en seguridad.	Oficial de seguridad de la información o quien haga sus veces.	Primera semana - Marzo 2025
2	Efectuar la revisión por la dirección del SGSI.	Comité institucional de gestión y desempeño.	Tercera semana - Marzo 2025
3	Generar informe de salidas de revisión por la dirección.	Comité institucional de gestión y desempeño.	Cuarta semana - Marzo 2025
4	Formalizar la solicitud de presupuesto en seguridad para el próximo periodo.	Oficial de seguridad de la información o quien haga sus veces.	Segunda semana - Abril 2025
5	Aprobación de presupuesto.	Alta dirección	Cuarta semana - Abril 2025

Fuente grupo TICS

7.2 PLAN DE ASEGURAMIENTO Y EVALUACIÓN DE LA IMPLEMENTACIÓN Y MANTENIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN

A continuación, se describe cómo realizar el seguimiento y evaluación de la implementación de Sistema de Gestión de Seguridad de la Información:

7.2.1 GESTIÓN DE INDICADORES

La gestión de indicadores permite evaluar la eficacia, eficiencia y efectividad de las políticas y controles de seguridad de la información implementados en el Ministerio de Minas y Energía. Basándonos en la **Guía Técnica No. 9** del MSPI y normativas internacionales como la **ISO/IEC 27001:2022** y la **ISO/IEC**

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

27004:2022, esta sección se enfoca en definir indicadores clave que apoyen la mejora continua y el cumplimiento normativo.

A continuación, se presentan los indicadores seleccionados y ajustados según las recomendaciones de la guía:

1. Indicadores de Organización y Gestión

- **SGIN01: Organización de Seguridad de la Información**
 - **Definición:** Mide el nivel de compromiso de la dirección con la asignación de roles y responsabilidades en seguridad.
 - **Fórmula:** $(\text{Número de roles definidos} / \text{Número total de roles requeridos}) * 100$
 - **Meta:** 80%-90% satisfactorio, 100% sobresaliente.

- **SGIN02: Cobertura del SGSI en activos de información**
 - **Definición:** Mide el porcentaje de activos críticos incluidos en el alcance del SGSI con controles implementados.
 - **Fórmula:** $(\text{Activos cubiertos} / \text{Total de activos críticos}) * 100$
 - **Meta:** 75%-80% mínimo, 100% sobresaliente.

2. Indicadores de Cumplimiento y Eficiencia

- **SGIN03: Tratamientos de eventos de seguridad**
 - **Definición:** Evalúa la eficiencia en la gestión de incidentes detectados.
 - **Fórmula:** $(\text{Eventos tratados} / \text{Eventos reportados}) * 100$
 - **Meta:** 80%-90% satisfactorio, 100% sobresaliente.

- **SGIN16: Implementación de controles**
 - **Definición:** Grado de avance en la implementación de controles definidos en el plan de tratamiento de riesgos.
 - **Fórmula:** $(\text{Controles implementados} / \text{Controles planificados}) * 100$
 - **Meta:** 75%-80% mínimo, 100% sobresaliente.

3. Indicadores de Disponibilidad y Resiliencia

- **SGIN13: Políticas de disponibilidad del servicio**

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- **Definición:** Grado de cumplimiento de políticas de continuidad operativa.
- **Fórmula:** (Servicios disponibles/Total de servicios planificados) * 100
- **Meta:** 100% sobresaliente.

- **SGIN15: Porcentaje de disponibilidad de servicios críticos**

- **Definición:** Porcentaje de tiempo que los sistemas críticos estuvieron disponibles según los ANS.
- **Fórmula:** (Tiempo disponible/Tiempo planificado) * 100
- **Meta:** >99% sobresaliente.

4. Indicadores de Cumplimiento Normativo

- **SGIN05: Cumplimiento de políticas de seguridad**

- **Definición:** Nivel de estructuración y adherencia a las políticas de seguridad definidas.
- **Fórmula:** Indicador binario (1 si cumple, 0 si no cumple).
- **Meta:** 100% cumplimiento.

5. Indicadores de Sensibilización y Cultura

- **SGIN04: Sensibilización en seguridad de la información**

- **Definición:** Efectividad del plan de sensibilización mediante auditorías o pruebas.
- **Fórmula:** (Eventos cumplidos/Total de eventos programados) * 100
- **Meta:** 80%-90% satisfactorio, 100% sobresaliente.

Tabla 7

Gestión de indicadores de seguridad de la información

Actividad	Responsable	Fecha de Inicio	Fecha de Finalización	Descripción
Definición de indicadores clave	Oficial de Seguridad o quien haga sus veces	Cuarta semana - Enero 2025	Primera semana - Febrero 2025	Selección de indicadores relevantes para el SGSI según normativas y metas.
Recolección inicial de datos	Oficial de Seguridad o quien haga sus veces	Segunda semana - Febrero 2025	Segunda semana - Marzo 2025	Establecimiento de líneas base para cada indicador clave.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Preparar el resultado de los indicadores para la revisión por la dirección.	Oficial de Seguridad o quien haga sus veces	Segunda semana - Marzo 2025	Cuarta semana - Marzo 2025	Primer informe de indicadores para iniciar hoja de ruta de mejora.
Efectuar la revisión por la dirección del SGSI.	Comité institucional de gestión y desempeño.	Segunda semana - Abril 2025	Segunda semana - Abril 2025	Detectar y aprobar cambios, ajustes y mejoras de los indicadores de gestión de seguridad de la información.
Realizar ajustes a los indicadores solicitadas por la revisión por la dirección.	Oficial de Seguridad o quien haga sus veces	Segunda semana - Abril 2025	Cuarta semana - Abril 2025	Según retroalimentación de la dirección del SGSI se hacen efectivos cambios sobre los indicadores.
Monitoreo y reportes trimestrales	Oficial de Seguridad o quien haga sus veces	Seguimiento trimestral	Seguimiento trimestral	Evaluación periódica de los resultados y elaboración de reportes.

Fuente grupo TICS

7.2.2 GESTIÓN DE VULNERABILIDADES

La gestión de vulnerabilidades es una parte esencial del Plan de Seguridad y Privacidad de la Información 2025, diseñada para identificar, evaluar y mitigar las debilidades en los sistemas de información y activos tecnológicos del Ministerio de Minas y Energía. Este proceso se fundamenta en estándares internacionales como la ISO/IEC 27001:2022, la ISO/IEC 27002:2022, y el NIST Cybersecurity Framework.

Las actividades a tener en cuenta para la gestión de vulnerabilidades técnicas se pueden consultar en la Tabla 8.

Tabla 8

Gestión de Vulnerabilidades Técnicas

Actividad	Responsable	Fecha de Inicio	Fecha de Finalización	Descripción
Diseño del formato de control	Oficial de Seguridad o quien haga sus veces	Cuarta semana - Enero 2025	Primera semana - Febrero 2025	Crear y validar el formato estándar para la documentación de vulnerabilidades.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Capacitación en uso del formato	Oficial de Seguridad o quien haga sus veces	Segunda semana - Febrero 2025	Segunda semana - Febrero 2025	Capacitar a los equipos en el uso del formato y su correcta documentación.
Elección y planeación de activos prioritarios	Oficial de Seguridad o quien haga sus veces / Grupo TICS	Cuarta semana - Febrero 2025	Cuarta semana - Febrero 2025	Establecer listado de prioridad de activos de información para gestión de vulnerabilidades
Ejecución de pruebas	Ingeniero de seguridad informática	Seguimiento semestral	Seguimiento semestral	Realizar escaneos y pruebas de penetración para identificar vulnerabilidades.
Documentación de hallazgos	Ingeniero de seguridad informática	Seguimiento semestral	Seguimiento semestral	Registrar los hallazgos en el formato de gestión de vulnerabilidades.
Planificación de remediación	Oficial de Seguridad o quien haga sus veces	Seguimiento trimestral	Seguimiento trimestral	Diseñar planes de acción para mitigar vulnerabilidades críticas y altas.
Ejecutar remediación	Equipo de desarrollo/ responsable del activo de información	Seguimiento trimestral	Seguimiento trimestral	Aplicar parches, reconfigurar sistemas o implementar controles compensatorios.
Pruebas de retest	Ingeniero de seguridad informática	Seguimiento trimestral	Seguimiento trimestral	Realizar pruebas para confirmar que las vulnerabilidades han sido mitigadas.
Monitoreo continuo	Ingeniero de seguridad informática	Constante	Constante	Revisión periódica para detectar nuevas vulnerabilidades o reincidencias.

Fuente grupo TICS

El pentesting anual es una simulación de ataque controlado diseñada para identificar vulnerabilidades en los sistemas y aplicaciones del Ministerio de Minas y Energía. Este proceso sigue un enfoque estructurado basado en las mejores prácticas internacionales y se encuentra estructurado dentro de la actividad de ejecución de pruebas, dicho proceso estará realizado por un proveedor de dicho servicio “Ethical hacking” bajo parámetros y alcances determinados por las partes. La siguiente tabla enmarca las tareas que se deberán cumplir respecto a dicho proceso:

Tabla 9

Actividades llevadas a cabo en la ejecución de pruebas de pentesting

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Actividad	Descripción
Definición del alcance	Identificar los sistemas, aplicaciones y redes críticas a evaluar.
Selección del proveedor	Contratar servicios de una firma externa certificada .
Revisión de contratos y NDA	Firmar acuerdos de confidencialidad (NDA) y definir límites legales y técnicos.
Planificación y diseño de pruebas	Crear un plan detallado que incluya metodologías, herramientas y cronograma.
Ejecución del pentesting	Realizar las pruebas en los entornos definidos sin interrumpir las operaciones.
Análisis de hallazgos preliminares	Presentar hallazgos iniciales y validar riesgos críticos con los responsables.
Entrega del informe final	Entregar un informe completo con vulnerabilidades, riesgos y recomendaciones.
Plan de remediación	Diseñar e implementar soluciones para mitigar las vulnerabilidades críticas.

Fuente grupo TICS

7.2.3 PLAN DE AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN

Para el SGSI se requiere realizar auditorías de seguridad para evidenciar el seguimiento y gestión del sistema, para ello se debe tener en cuenta lo siguiente:

Objetivo de la auditoría: Revisar el funcionamiento y mantenimiento del Sistema de Gestión de Seguridad de la Información del MINENERGÍA.

Alcance de la auditoría: El alcance de la auditoría abarca a todo el MINENERGÍA y sus procesos, teniendo como base de revisión la norma ISO 27001:2013 y el Modelo de Seguridad y Privacidad de la información de MINTIC. Los procesos por auditar son:

- Direccionamiento estratégico y control internacional.
- Gestión internacional.
- Administración del sistema integrado de gestión.
- Comunicación institucional.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- e) Formulación y adopción de planes, programas, reglamentos y lineamientos sectoriales.
- f) Ejecución de políticas, proyectos y reglamentación sectorial.
- g) Seguimiento, vigilancia y control a políticas, planes, programas, proyectos y reglamentación sectorial.
- h) Gestión de talento humano.
- i) Gestión documental.
- j) Gestión financiera.
- k) Gestión tecnológica, de información y comunicación.
- l) Gestión de recursos físicos.
- m) Gestión jurídica.
- n) Auditoría y evaluación.
- o) Control interno disciplinario.
- p) Servicio al ciudadano.

Criterios de auditoría: Normatividad vigente que aplique a la fecha, así mismo las Políticas, Procedimientos, Instructivos, Planes, Mapas de Riesgos de Seguridad de la Información, Informe de Revisión por la Dirección y el Plan de Seguridad de la información.

Tabla 10

Plan de Auditorías de Seguridad de la Información

NO	Actividades	Responsable	Fecha
1	Establecimiento del perfil del equipo auditor.	Oficina de Control Interno	Primera semana-Febrero 2025
2	Definición del grupo auditor.	Oficina de Control Interno	Tercera semana -Febrero 2025
3	Generar el listado de procesos a auditar con la fecha y hora en la que se realizará la auditoría (Instrumento de evaluación del MSPI de MINTIC, análisis de riesgos, revisión por la dirección, políticas de seguridad, etc.).	Oficina de Control Interno	Primera semana -Marzo 2025

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

4	Entrega de listado de información a entregar al auditor previa ejecución de la auditoría.	Oficina de Control Interno	Segunda semana - Marzo 2025
5	Reunión de Apertura de Auditoría	Auditor	Segunda semana - Abril 2025
6	Ejecución de auditoría.	Auditor	Tercera semana - Cuarta semana - Abril 2025
7	Reunión de Cierre de auditoría	Auditor	Cuarta semana - Abril 2025
8	Redacción de informe de auditoría	Auditor	Segunda semana - Mayo 2025
9	Presentación de informe de auditoría	Auditor	Tercera semana - Mayo 2025
10	Plan de subsanación de no conformidades.	Administradores de los sistemas de información en conjunto con el Oficial de Seguridad de la información o quien haga sus veces.	Primera semana - Junio 2025

Fuente grupo TICS

7.2.4 PLAN DE MEJORAMIENTO CONTINUO

El mejoramiento continuo de seguridad de la información está estrechamente ligado a la ejecución de auditorías, con base en la auditoría realizada para el periodo se deben ejecutar las siguientes actividades una vez se cuente con el informe de auditoría:

Tabla 11

Mejoramiento Continuo

NO	Actividades	Responsable	Fecha
----	-------------	-------------	-------

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1	Identificar las no conformidades documentadas en el informe de auditoría.	Oficial de seguridad de la información o quien haga sus veces.	Primera semana - Abril 2025
2	Evaluar las necesidades de acciones para eliminar las causas de la no conformidad con el fin de que no vuelva a ocurrir.	Oficial de seguridad de la información o quien haga sus veces.	Tercera semana - Abril 2025
3	Establecer las acciones para controlar y corregir las no conformidades.	Oficial de seguridad de la información o quien haga sus veces.	Primera semana - Mayo 2025
4	Ejecutar las acciones para controlar y corregir las no conformidades.	Oficial de seguridad de la información o quien haga sus veces.	Tercera semana - Mayo 2025
5	Revisar la eficacia de las acciones correctivas tomadas.	Oficial de seguridad de la información o quien haga sus veces.	Tercera semana - Agosto 2025
6	Realizar los cambios al SGSI de ser necesario.	Oficial de seguridad de la información o quien haga sus veces.	Tercera semana - Septiembre 2025
7	Establecer un mecanismo de contacto para las sugerencias de las partes interesadas que propongan mejoras al SGSI.	Oficial de seguridad de la información o quien haga sus veces.	Tercera semana - Octubre 2025
8	Implementar el mecanismo de contacto para las sugerencias de las partes interesadas que propongan mejoras al SGSI.	Oficial de seguridad de la información o quien haga sus veces.	Segunda semana - Noviembre 2025

Fuente grupo TICS

7.2.5 REVISIÓN POR LA ALTA DIRECCIÓN

La revisión por la dirección debe ejecutarse a intervalos planificados; para ello se debe tener como entrada lo siguiente:

- a) Estado de las acciones con relación a las revisiones previas por la dirección.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- b) Cambios en cuestiones externas e internas que le apliquen al SGSI.
- c) Realimentación sobre el desempeño de la Seguridad de la Información.
- d) Resultados de la auditoría.
- e) Realimentación de las partes interesadas.
- f) Resultados del análisis y tratamiento de riesgos.
- g) Oportunidades de mejora continua.

Las actividades a tener en cuenta para la revisión por la dirección se pueden consultar en la **Tabla 12**.

Tabla 12

Revisión por la Dirección

No	Descripción de la actividad	Responsable	Fecha
1	Alistamiento de las entradas para la revisión por la dirección.	Oficial de Seguridad de la información o quien haga sus veces.	Primera semana - Junio 2025
2	Ejecución de la revisión por la dirección.	Comité institucional de gestión y desempeño.	tercera semana - Junio 2025
3	Redacción de informe de la revisión por la dirección.	Comité institucional de gestión y desempeño.	Cuarta semana - Junio 2025

Fuente grupo TICS

7.3 PLAN DE COMUNICACIONES

A continuación, se detalla el plan de comunicaciones de seguridad.

7.3.1 CARACTERIZACIÓN DE INTERESADOS

La caracterización de interesados permite identificar y comprender los grupos que interactúan con el Plan de Seguridad y Privacidad de la Información 2025, garantizando una comunicación efectiva y adaptada a sus necesidades. Basándonos en la información proporcionada, aquí se organiza y estructura la caracterización de los grupos de interés.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Descripción de las Categorías

1. Internos y Externos:

- **Internos:** Personal vinculado directamente al Ministerio (funcionarios, contratistas, directivos, accionistas, etc.).
- **Externos:** Clientes, proveedores, entidades financieras, sindicatos, comunidad local, organizaciones sociales, etc.

2. Primarios y Secundarios:

- **Primarios:** Actores claves directamente afectados por las decisiones o acciones del Plan.
- **Secundarios:** Actores que tienen interés o influencia indirecta en las decisiones del Plan.

Tabla 13

Caracterización de Interesados

Grupo de Interés	Descripción	Características	Necesidades Clave	Frecuencia de Comunicación
Ministra o ministro del MINENERGÍA	Personal que trabaja directamente con el(la) ministro(a) del MINENERGÍA.	- Internos.	Reportes ejecutivos, decisiones estratégicas.	Mensual.
		- Primarios.		
Comité Institucional de Gestión y Desempeño	Grupo encargado de implementar y desarrollar las políticas de gestión del MIPG, según el Decreto 1499 de 2017.	- Internos.	Políticas de gestión, actualizaciones normativas.	Trimestral.
		- Primarios.		
Colaboradores de TI	Colaboradores que trabajan en la Gerencia de Tecnologías de la Información.	- Internos y externos.	Capacitación en políticas y procedimientos.	Según necesidad.
		- Primarios y secundarios.		
Oficina de planeación y gestión organizacional	Colaboradores de la Gerencia de Planeación Institucional.	- Internos y externos.	Directrices para la alineación estratégica.	Mensual.
		- Primarios y secundarios.		

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Oficina de Control Interno	Personal de la Oficina de Control Interno.	- Internos.	Reportes de cumplimiento, auditorías.	Trimestral.
		- Primarios.		
Ciudadanos	Ciudadanos de Colombia que interactúan con los servicios del Ministerio.	- Externos.	Transparencia en políticas y seguridad.	Anual o según eventos.
		- Secundarios.		
Todos los colaboradores del MINENERGÍA	Funcionarios y contratistas del Ministerio de Minas y Energía.	- Internos y externos.	Sensibilización, cumplimiento de políticas.	Trimestral.
		- Primarios y secundarios.		
Secretaría General	La(o) secretaria(o) general del MINENERGÍA.	- Internos.	Información estratégica y de alto nivel.	Mensual.
		- Primarios.		

Fuente grupo TICS

7.3.2 COMUNICACIONES

La comunicación es un componente crítico para garantizar que la Seguridad de la Información cumpla con los objetivos establecidos en el Ministerio de Minas y Energía. Una gestión de comunicaciones efectiva no solo asegura que los mensajes lleguen a los grupos de interés adecuados, sino que también fomenta la comprensión y el cumplimiento de las políticas, procedimientos y lineamientos establecidos.

Para lograr resultados óptimos, es necesario:

1. Definir claramente los documentos a comunicar:

- Identificar los documentos clave que deben ser difundidos, como políticas de seguridad, manuales de procedimientos, reportes de cumplimiento y alertas sobre amenazas emergentes.
- Asegurar que cada documento esté alineado con las necesidades de los grupos de interés definidos previamente (ver **Tabla 13**).

2. Especificar los aspectos inherentes a la comunicación:

- **Canal:** Seleccionar medios efectivos y accesibles para cada grupo de interés, como correos electrónicos, reuniones, portales web internos y boletines.
- **Formato:** Utilizar formatos claros y adaptados según la naturaleza del mensaje.
- **Responsable:** Asignar responsables específicos para cada tipo de comunicación, asegurando que los mensajes sean precisos y oportunos.
- **Frecuencia:** Establecer cronogramas de comunicación regulares que permitan mantener informados a los interesados, así como comunicaciones ad-hoc en respuesta a eventos críticos.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Tabla 14

Enfoque de las comunicaciones

Mensaje	Grupo de interés	Canal	Formato	Responsable	Frecuencia
Políticas y procedimientos de seguridad	Comité Institucional de Gestión y Desempeño	Reunión de comité-presencial/virtual	.DOC	Oficial de Seguridad de la información o quien haga sus veces.	Anual o cada vez que se cree o modifique una política o procedimiento
	Todos los colaboradores del MINENERGÍA	Página oficial del Ministerio	.PDF		
Sensibilización en seguridad	Todos los colaboradores del MINENERGÍA	Charlas, conferencias, capacitaciones.	.PPT	Oficial de Seguridad de la Información o quien haga sus veces.	Mensual
Análisis de riesgos	Comité Institucional de Gestión y Desempeño	Herramienta GRC (Gobierno, Riesgo y Cumplimiento)	Según plataforma	Oficial de Seguridad de la información o quien haga sus veces.	Anual
	Oficina de planeación y gestión organizacional				
	Oficina de Control Interno				
	Ministra o ministro del MINENERGÍA				
	Todos los colaboradores del MINENERGÍA				
Incidentes de seguridad	Comité Institucional de Gestión y Desempeño	Correo electrónico con informe del incidente	.PDF	Oficial de Seguridad de la información o quien haga sus veces.	Cada vez que se requiera.
	Ministra o ministro del MINENERGÍA				
	Secretaría General				
Comunicados de prensa	Ciudadanos	Entrevista	Impreso y/o audiovisual	Secretaría General	Cada vez que se requiera.

Fuente grupo TICS

7.4 PLAN DE SENSIBILIZACIÓN Y CAPACITACIÓN

La sensibilización y capacitación en seguridad de la información es un componente esencial para garantizar que los usuarios comprendan su rol en el mantenimiento de la confidencialidad, integridad,

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

disponibilidad y privacidad de la información dentro del Ministerio de Minas y Energía. Este plan se basa en el Procedimiento de Capacitación y Sensibilización de Personal, y busca fomentar una cultura organizacional de seguridad, alineada con los objetivos del Plan de Seguridad y Privacidad de la Información 2025.

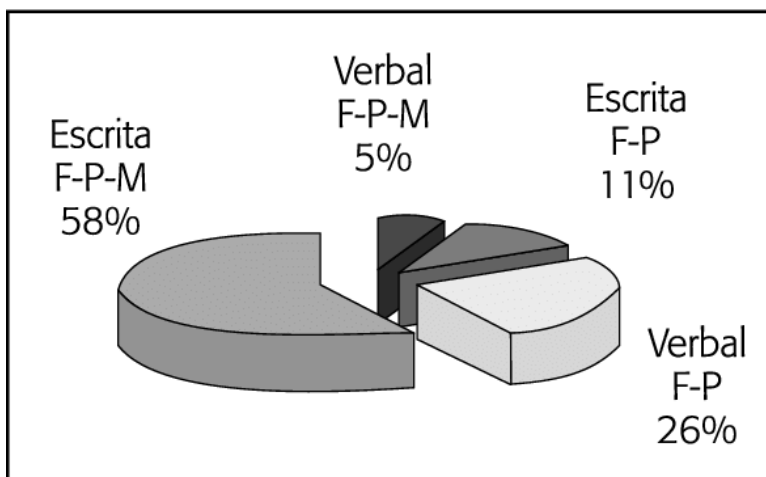
7.4.1 SENSIBILIZACIÓN

La sensibilización en seguridad de la información es un componente esencial para construir una cultura organizacional que valore la protección de los datos y activos tecnológicos. Este proceso busca aprovechar la comunicación asertiva como herramienta clave para generar conciencia en los colaboradores del Ministerio de Minas y Energía, alineándolos con los objetivos del SGSI.

La comunicación, como una de las actividades más frecuentes y esenciales del ser humano, requiere un enfoque planificado y asertivo para maximizar su efectividad. Según Rankin (citado por McEntee, 1988), más del 60% de las actividades diarias de las personas involucran algún tipo de comunicación. Este dato refuerza la necesidad de diseñar mensajes claros y estratégicos que impacten positivamente en la comprensión y el comportamiento de los colaboradores.

En el contexto del SGSI, la comunicación asertiva permite:

1. **Maximizar la recepción de mensajes clave:** Asegurando que los colaboradores comprendan la importancia de la seguridad de la información y su rol en la organización.
2. **Fomentar el compromiso:** Involucrando a todos los niveles jerárquicos en la adopción de prácticas seguras.
3. **Reducir resistencias al cambio:** Al presentar los beneficios de una cultura de seguridad en términos prácticos y comprensibles.



Fuente: Rankin, citado por McEntee. *Comunicación Oral*. Alhambra Editorial, 1988

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

7.4.1.1 MODALIDAD

El siguiente paso, es seleccionar la modalidad más acorde con el tipo de información a comunicar, entre las diferentes opciones con las que cuenta la Entidad, se encuentran:

- a) **E-card:** Consiste en diseñar una tarjeta virtual llamativa, con poco texto y más imágenes, esta modalidad es más efectiva a la hora de transmitir mensajes muy puntuales y concisos.
- b) **Infografía:** es una representación gráfica que pretende explicar o resumir una información, combinando iconos como imágenes, gráficos, etc. con descripciones, narraciones, interpretaciones y datos. Son interpretaciones visuales de los propios textos y resultan más atractivas para el lector.
- c) **Videos animados:** Consiste en diseñar presentaciones animadas y videos explicativos animados muy cortos de máximo de 5 minutos de duración.
- d) **Papel tapiz:** Conocido además como **wallpaper**, fondo de escritorio o fondo de pantalla, se trata de la fotografía o la ilustración que el administrador de una computadora (ordenador), escoge como fondo de la pantalla.
- e) **Cartillas:** es una revista corta de un tema específico, cuyo propósito es orientar sobre un tema de interés.
- f) **Folletos:** es un texto impreso en pequeñas hojas de diferentes formas que sirve como una herramienta publicitaria, cuyo propósito es invitar a la audiencia a profundizar en un tema de interés.
- g) **Landing page (o páginas de aterrizaje):** es una página Web a la que llegarán los usuarios al hacer clic en un Link de una publicación o de una pieza de sensibilización en concreto.
- h) **Newsletter** (o boletín informativo): es una publicación distribuida de forma regular, centrada en un tema principal.

7.4.1.2 MEDIOS

Para garantizar que los mensajes de seguridad de la información sean recibidos de manera eficaz, el Ministerio debe seleccionar y adaptar los medios de comunicación de acuerdo con los diferentes grupos de interés, la naturaleza de los temas a tratar y la etapa de madurez del SGSI. La comunicación debe ser oportuna, clara y accesible, utilizando canales electrónicos como correo electrónico, combinados con métodos presenciales como talleres interactivos, y soportados por medios visuales como infografías y videos educativos. Es importante que la comunicación sea continua y bidireccional, permitiendo la retroalimentación de los colaboradores y ajustando las estrategias según los resultados obtenidos.

- a) **Correo:** Se trata del correo institucional en Microsoft Teams con dominio minienergia.gov.co establecido por la Entidad para todos los comunicados oficiales.
- b) **Portal web:** Se trata de la página web oficial: <https://www.MINENERGÍA.gov.co/> de la Entidad.
- c) **Pantallas:** Se trata de pantallas ubicadas en diferentes sitios estratégicos de la Entidad para su consulta en sitio.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Finalmente, el Oficial de Seguridad de la Información o quien haga sus veces procede a asignar las fechas en las que se debe emitir cada pieza grafica teniendo en cuenta la periodicidad establecida en el cronograma para la sensibilización.

7.4.2 CAPACITACIÓN

La capacitación es un proceso estructurado y más profundo que la sensibilización, y está orientado a proporcionar a los colaboradores las habilidades y conocimientos necesarios para gestionar de manera efectiva los riesgos relacionados con la seguridad de la información (GTC ISO/IEC 27005:2015). A través de la capacitación, el Ministerio de Minas y Energía busca garantizar que el personal no solo comprenda la importancia de la seguridad de la información, sino que también pueda aplicar procedimientos específicos para proteger los activos de información de la organización.

La capacitación debe incluir módulos formales, tanto presenciales como en línea, que cubran los aspectos técnicos y operativos de la seguridad de la información. Esto incluye, entre otros, el uso de herramientas de protección, la gestión de incidentes de seguridad, el cumplimiento de normativas internas y externas, y la protección de infraestructuras críticas. Además, se debe proporcionar formación continua, adaptada a la evolución de las amenazas, las tecnologías emergentes y las actualizaciones normativas.

7.4.2.1 DEFINICIÓN DE PÚBLICOS OBJETIVO

No todos los usuarios se deben capacitar en los mismos temas ni con el mismo enfoque, de ahí la importancia de identificar primero las necesidades de capacitación y luego consolidar los diferentes grupos de usuarios que se requiere reforzar con los temas seleccionados. Entre los diferentes públicos objetivo a tener en cuenta, pero sin limitarse a este listado, se encuentran:

- a) Ministro y directores.
- b) Jefes de oficina y coordinadores.
- c) Líderes de proceso.
- d) Comité institucional de gestión y desempeño.
- e) Oficial de seguridad de la información.
- f) Profesionales de seguridad de la información.
- g) Grupo de soporte informático.
- h) Propietarios de la información.
- i) Responsable del riesgo.

7.4.2.2 MODALIDAD

El siguiente paso, es seleccionar la modalidad más acorde con el tipo de capacitación a dictar y las normas sanitarias vigentes en su momento, entre las diferentes opciones con las que cuenta la Entidad, se encuentran:

- a) **Presencial:** Catedra dirigida en las instalaciones de la Entidad.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- b) **Virtual:** Catedra dirigida y realizada por medio de herramientas virtuales de comunicación como lo son Google meet, Microsoft teams, entre otros.
- c) **Estudio autónomo:** Consiste en sesiones organizadas por módulos y pre cargadas en herramientas de aprendizaje para que los usuarios realicen los cursos sin la presencia del catedrático.

7.4.2.3 MEDIOS

Talleres y Seminarios Presenciales

- **Descripción:** Sesiones cara a cara donde los empleados pueden interactuar con formadores expertos, realizar actividades prácticas y resolver dudas en tiempo real.
- **Ventajas:**
 - Promueve la participación activa y la colaboración en equipo.
 - Permite la resolución de problemas prácticos mediante simulaciones de incidentes.

Webinars y Conferencias Virtuales

- **Descripción:** Sesiones en línea que reúnen a expertos y empleados para tratar temas específicos de seguridad de la información, generalmente en formato de presentación con espacio para preguntas y respuestas.
- **Ventajas:**
 - Mayor alcance, ya que pueden incluir a empleados de diferentes ubicaciones.
 - Flexibilidad de horarios y accesibilidad a la grabación para revisarla posteriormente.

7.4.2.4 CAPACITACIÓN BASADA EN UN EJERCICIO DE CRISIS

La capacitación basada en un ejercicio o escenario de crisis es un componente clave para visualizar y hacer reconocimiento de como el Ministerio de Minas y Energía está preparado para responder de manera efectiva ante situaciones imprevistas relacionadas con la seguridad de la información. Este tipo de capacitación, que simula una crisis real, permite a los participantes aplicar sus conocimientos y habilidades en un entorno controlado y práctico, mejorando su capacidad para manejar situaciones críticas de forma ágil y eficaz.

Esta metodología tiene como objetivo poner a prueba la capacidad de los colaboradores para responder ante incidentes de seguridad de la información, como ciberataques, filtraciones de datos o fallos en la infraestructura crítica. Utilizando simulaciones realistas, los empleados practican la gestión de incidentes en tiempo real, tomando decisiones y colaborando en equipo para mitigar los efectos de la crisis. Se fundamenta en las recomendaciones de las normativas internacionales como ISO/IEC 27001:2022, que promueve la gestión de incidentes y la recuperación ante desastres, y el NIST Cybersecurity Framework, que enfatiza la importancia de la resiliencia organizacional y la preparación

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

para ciberincidentes. Además, el MSPI establece los lineamientos y guía adecuada de la valoración, gestión y respuesta ante incidentes de seguridad de la información (contención, erradicación y recuperación).

Elementos clave del ejercicio de crisis:

1. **Simulación de un incidente real:** Ejercicios prácticos de ataques cibernéticos, violaciones de datos, o problemas técnicos en infraestructuras críticas.
2. **Participación activa:** Involucrar a los responsables de áreas clave (TI, seguridad de la información, comunicaciones, dirección) para probar la capacidad de respuesta colectiva.
3. **Evaluación en tiempo real:** Monitorear y evaluar las decisiones tomadas durante el ejercicio, proporcionando retroalimentación inmediata sobre la gestión del incidente.
4. **Recuperación de la situación:** Asegurar que los participantes practiquen los protocolos de recuperación y restauración de servicios esenciales después de un incidente.

Tabla 15

Cronograma de gestión de escenario de crisis

Actividad	Responsable	Fecha de Inicio	Fecha de Finalización	Descripción
Definición del escenario de crisis	Oficial de Seguridad o quien haga sus veces /Gestión de riesgos	Primera semana - Marzo 2025	Segunda semana - Marzo 2025	Determinar el tipo de incidente a simular (e.g., ciberataque, filtración de datos). Definir el impacto y las áreas involucradas.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Desarrollo de los procedimientos del ejercicio	Oficial de Seguridad o quien haga sus veces /Gestión de riesgos	Segunda semana - Marzo 2025	Segunda semana - Abril 2025	Elaborar los protocolos y guías de respuesta, los roles de los participantes y los resultados esperados del ejercicio.
Planificación de la logística	Grupo TICS	Segunda semana - Abril 2025	Cuarta semana - Mayo 2025	Organizar los recursos necesarios para el ejercicio (infraestructura, equipos, acceso).
Simulación del ejercicio	Oficial de Seguridad o quien haga sus veces /Gestión de riesgos	Cuarta semana - Mayo 2025	Segunda semana - Junio 2025	Realizar la simulación del incidente en un entorno controlado. Evaluar las respuestas y las decisiones tomadas.
Evaluación y retroalimentación	Oficial de Seguridad o quien haga sus veces /Gestión de riesgos	Finalizando ejercicio de crisis	Finalizando ejercicio de crisis	Evaluar el desempeño del ejercicio, identificar áreas de mejora y generar un informe detallado con recomendaciones.
Ajustes a políticas y procedimientos	Oficial de Seguridad o quien haga sus veces /Gestión de riesgos	Segunda semana - Julio 2025	Segunda semana - Julio 2025	Revisar y ajustar las políticas y procedimientos de seguridad en función de los resultados del ejercicio.

Fuente grupo TICS

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Beneficios del ejercicio de crisis

1. **Mejora en la capacidad de respuesta:** Los empleados adquieren experiencia práctica en situaciones de alta presión, lo que mejora su capacidad para manejar incidentes reales.
2. **Identificación de debilidades:** El ejercicio pone al descubierto posibles fallos en la infraestructura, las políticas o las respuestas de los equipos, permitiendo realizar ajustes antes de que ocurra un incidente real.
3. **Refuerzo de la resiliencia organizacional:** Fortalece la preparación del Ministerio para responder rápidamente ante incidentes, minimizando los impactos operativos y financieros.

7.4.2.1 SELECCIÓN DE TEMAS

Inicialmente, el Ministerio debe seleccionar los temas que, dependiendo de la etapa de madurez en la que se encuentre el SGSI, sean prioritarios para comunicar y fortalecer. La selección debe alinearse con estándares internacionales como la ISO/IEC 27002:2022 y la normativa nacional MSPI, y estar enfocada en fortalecer la cultura organizacional de seguridad.

Tabla 16

Temas propuestos y adaptables al plan de seguridad y privacidad de la información en sensibilización y capacitación

Categoría	Tema	Descripción
Fundamentales	Política general de Seguridad de la Información	Importancia y alineación con los objetivos estratégicos del Ministerio.
	Responsabilidades en Seguridad de la Información	Roles claros y mecanismos para cumplir con dichas responsabilidades.
	Políticas y procedimientos clave	Gestión de contraseñas, uso seguro de dispositivos móviles y protección de datos personales.
	Reglas y obligaciones de seguridad aplicables	Cumplimiento de leyes, normativas internas y estándares internacionales.
	Rendición de cuentas y consecuencias	Implicaciones legales y organizativas de incumplir políticas de seguridad.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

	Puntos de contacto y recursos adicionales	Identificación de contactos internos y externos para dudas o incidentes de seguridad.
	Gestión de incidentes y ciberseguridad	Procedimientos básicos para identificar, reportar y responder a amenazas.
	Clasificación y etiquetado de información	Correcta identificación y manejo seguro de información según su nivel de confidencialidad.
	Seguridad física de activos de información	Estrategias para proteger equipos críticos frente a accesos no autorizados.
	Cifrado de información	Uso de cifrado en correos, documentos y comunicaciones.
Avanzados y Emergentes	Riesgos de la inteligencia artificial	Concienciar sobre usos maliciosos de IA, como deepfakes o ataques automatizados.
	Resiliencia ante ataques de denegación de servicio (DDoS)	Medidas preventivas para mitigar este tipo de ataques.
	Identificación de ransomware y procedimientos de respuesta	Cómo detectar señales de ransomware y responder ante una infección.
	Gestión de dispositivos BYOD (Bring Your Own Device)	Normas para el uso seguro de dispositivos personales en el entorno corporativo.
	Seguridad en redes sociales corporativas	Prácticas seguras para manejar cuentas oficiales y personales relacionadas con la organización.
Sectoriales y Específicos	Protección de infraestructuras críticas	Protocolos para sistemas estratégicos del sector energético y minero.
	Integridad en la cadena de suministro digital	Gestión de riesgos con proveedores y terceros que manejan información del Ministerio.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

	Gestión de riesgos en servicios en la nube	Buenas prácticas y requisitos para proteger datos en IaaS, PaaS y SaaS.
	Seguridad en proyectos de transición energética	Identificación de riesgos tecnológicos en iniciativas de energía renovable.
	Introducción a normativas internacionales	Aspectos clave de la ISO/IEC 27701 (Privacidad) y 22301 (Continuidad).
	Actualizaciones del SGSI	Cambios en políticas, procedimientos o evaluaciones de riesgos.
Basados en Fuentes	Incidentes de Seguridad de la Información	Temas derivados de lecciones aprendidas en incidentes recientes.
	Resultados de campañas anteriores	Áreas de mejora identificadas en sensibilizaciones previas.
	Auditorías internas y externas	Incorporación de recomendaciones derivadas de revisiones técnicas.
	Amenazas externas y tendencias globales	Reportes de ENISA, NIST y OWASP sobre ciberseguridad.
	Normativa vigente y actualizaciones	Cambios en leyes nacionales y estándares internacionales aplicables.
	Días internacionales de ciberseguridad	Fechas relevantes para promover actividades temáticas.
	Informes internacionales	Referencias internacionales

Fuente grupo TICS

8. RECOMENDACIONES

- Desarrollar y mantener actualizadas las políticas y procedimientos de seguridad, asegurando su alineación con las normativas nacionales e internacionales aplicables.
- Incluir lineamientos específicos para la protección de infraestructuras críticas y sistemas específicos del sector energético y minero.
- Implementar programas regulares de capacitación para todos los niveles de la organización, desde la Alta Dirección hasta el personal operativo.
- Adaptar los temas de capacitación a riesgos emergentes y actualizaciones normativas.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Realizar evaluaciones periódicas de riesgos en los sistemas de información y activos críticos.
- Priorizar la implementación de controles sobre los riesgos identificados como de mayor criticidad.
- Establecer un proceso estructurado para la identificación, análisis, respuesta y recuperación ante incidentes de seguridad.
- Simular escenarios de crisis para evaluar la efectividad de los planes de respuesta.
- Implementar herramientas de monitoreo para identificar amenazas en tiempo real y prevenir incidentes.
- Analizar tendencias y comportamientos anómalos en los sistemas de información.

9. MEJORES PRÁCTICAS

Las mejores prácticas en seguridad de la información constituyen un conjunto de recomendaciones basadas en estándares internacionales, diseñadas para abordar los riesgos modernos y proteger los activos críticos de la organización. La ISO/IEC 27002:2022 destaca por su enfoque actualizado en controles específicos organizados en categorías como organizacional, tecnológica, física y de personas, brindando herramientas efectivas para mitigar amenazas y garantizar la resiliencia operativa. Entre los aspectos clave de este estándar se encuentran la gestión de incidentes, el monitoreo continuo y la implementación de controles tecnológicos avanzados, como el cifrado y la autenticación multifactorial.

El NIST Cybersecurity Framework 2.0 (2024) introduce un modelo estratégico que enfatiza la gobernanza, la detección proactiva de amenazas y la recuperación efectiva tras incidentes. Sus seis funciones principales —Govern, Identify, Protect, Detect, Respond y Recover— proporcionan un enfoque integral para gestionar riesgos cibernéticos y alinear la ciberseguridad con los objetivos estratégicos de la organización. Adicionalmente, publicaciones como la NIST 800-53 y la NIST 800-82 ofrecen controles específicos para sistemas federales y de control industrial, respectivamente, áreas críticas para sectores como el energético y minero.

Finalmente, las prácticas basadas en la ISO/IEC 31000 y el NIST 800-39 refuerzan la gestión integral de riesgos mediante la evaluación continua de amenazas y el diseño de arquitecturas de seguridad resilientes. Estas incluyen estrategias como la segmentación de redes, la automatización de respuestas mediante inteligencia artificial y el uso del enfoque de confianza cero (Zero Trust), garantizando una protección sólida frente a los desafíos del entorno digital actual. Estas recomendaciones permiten al Ministerio de Minas y Energía adaptarse proactivamente a las demandas normativas y operativas del sector.

10. GLOSARIO

A

- **Activo:** Cualquier cosa que tiene valor para la organización, incluyendo información, hardware, software, personal, reputación y servicios. (ISO/IEC 27000:2023)
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar su nivel en función de los objetivos organizacionales. (ISO/IEC 31010:2019)

B

- **BIA (Business Impact Analysis):** Proceso para analizar las funciones críticas de negocio y el impacto que tendría su interrupción en las operaciones de la organización. (ISO/IEC 22301:2019)

C

- **Confidencialidad:** Propiedad que asegura que la información solo esté disponible para quienes están autorizados a acceder a ella. (ISO/IEC 27000:2023)
- **Ciberseguridad:** Práctica de proteger los sistemas conectados a Internet, incluidos hardware, software y datos, de ciberataques. (NIST CSF 2.0, 2024)

D

- **Disponibilidad:** Garantizar que la información y los sistemas estén accesibles y utilizables por quienes los necesiten, en el momento que los necesiten. (ISO/IEC 27000:2023)

E

- **Evaluación del Riesgo:** Proceso de comparar los riesgos identificados contra los criterios establecidos para determinar la importancia del riesgo. (ISO/IEC 31000:2018)

G

- **Gestión del Riesgo:** Conjunto de actividades coordinadas para identificar, evaluar y controlar los riesgos dentro de una organización. (ISO/IEC 31000:2018)
- **Gobernanza de Seguridad de la Información:** Marco estratégico que define cómo se gestiona la seguridad de la información en una organización, alineada con los objetivos de negocio. (NIST CSF 2.0, 2024)

M

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- **MSPI (Modelo de Seguridad y Privacidad de la Información):** Enfoque integral para proteger los sistemas de información y datos organizacionales en Colombia, alineado con las políticas nacionales y estándares internacionales.

P

- **Política:** Declaración formal de la Alta Dirección que establece las directrices para el manejo de la seguridad de la información. (ISO/IEC 27001:2022)
- **Plan de Tratamiento de Riesgos:** Documento que define las acciones necesarias para mitigar los riesgos identificados y proteger la información organizacional. (ISO/IEC 27001:2022)

R

- **Riesgo:** Efecto de la incertidumbre sobre los objetivos organizacionales. (ISO/IEC 31000:2018)
- **Resiliencia Organizacional:** Capacidad de una organización para adaptarse a los cambios y responder efectivamente a incidentes que afectan sus operaciones. (ISO/IEC 22301:2019)

S

- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, incluyendo aspectos de autenticidad, responsabilidad, privacidad y no repudio. (ISO/IEC 27000:2023)
- **SGSI (Sistema de Gestión de Seguridad de la Información):** Enfoque sistemático basado en políticas, procedimientos y controles para gestionar riesgos relacionados con la seguridad de la información. (ISO/IEC 27001:2022)
- **SIGME (Sistema Integrado de Gestión del Ministerio de Minas y Energía):** Sistema que integra los diferentes procesos organizacionales para optimizar la gestión administrativa, técnica y operativa del Ministerio, asegurando el cumplimiento de sus objetivos estratégicos.

T

- **Tratamiento del Riesgo:** Proceso para seleccionar e implementar medidas destinadas a modificar el riesgo. (ISO/IEC 31000:2018)

V

- **Vulnerabilidad:** Debilidad en un activo o control que puede ser explotada por una amenaza. (ISO/IEC 27000:2023)

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

11. REFERENCIAS

Normas Internacionales

1. **ISO/IEC 27001:2022**: Especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).
2. **ISO/IEC 27002:2022**: Proporciona directrices sobre la implementación de controles de seguridad de la información.
3. **ISO/IEC 27701:2019**: Extensión de la ISO/IEC 27001 para la gestión de la privacidad y protección de datos personales.
4. **ISO/IEC 22301:2019**: Norma para la gestión de la continuidad del negocio.
5. **ISO/IEC 31000:2018**: Marco para la gestión de riesgos organizacionales.
6. **ISO/IEC 27005:2022**: Guía para la gestión del riesgo en la seguridad de la información.

Publicaciones del NIST

1. **NIST Cybersecurity Framework (CSF) 2.0, 2024**: Marco actualizado para la gestión de riesgos de ciberseguridad con seis funciones clave.
2. **NIST SP 800-39**: Guía para la gestión integrada de riesgos en seguridad cibernética.
3. **NIST SP 800-53 Rev. 5**: Controles de seguridad y privacidad para sistemas de información federales.
4. **NIST SP 800-82 Rev. 2**: Guía para la seguridad de sistemas de control industrial (ICS).
5. **NIST SP 800-207**: Modelo de seguridad basado en la filosofía Zero Trust.

Normas y Guías Nacionales

1. **MSPI (Modelo de Seguridad y Privacidad de la Información)**: Estándar colombiano para la gestión de la seguridad y privacidad en las entidades públicas.
2. **Resolución 40646 de 2023 (MinMinas)**: Define el marco de las políticas de seguridad de la información para el Ministerio de Minas y Energía.
3. **Ley 1581 de 2012**: Régimen general de protección de datos personales en Colombia.
4. **Guía DAFP**: Guía para la administración y gestión del riesgo, emitida por el Departamento Administrativo de la Función Pública.