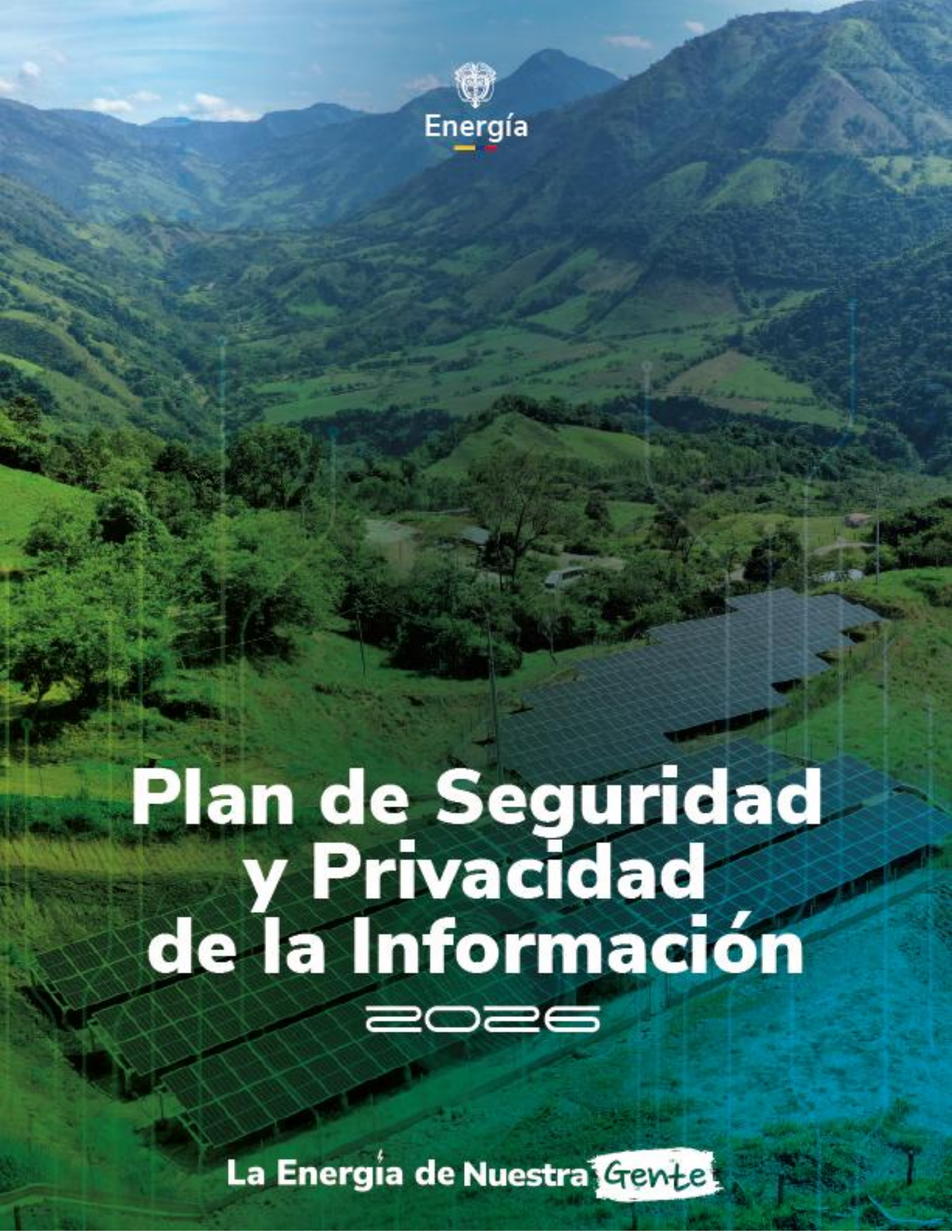

Energía
Plan de Seguridad y Privacidad de la Información
2026
La Energía de Nuestra Gente

VERSIÓN EN REVISIÓN

FECHA 08/12/2025

APROBACIONES

ELABORÓ		REVISÓ		APROBÓ	
Cargo:	Seguridad de la información	Cargo:	Profesional Especializado	Cargo:	
Dependencia:	Grupo TICS	Dependencia:	Grupo TICS	Dependencia:	OPGI
Fecha:	08/12/2025	Fecha:		Fecha:	

Fuente: MINENERGÍA

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

La transformación digital acelerada por la pandemia de COVID-19 consolidó en las entidades públicas colombianas una dependencia estratégica de los sistemas de información y la adopción masiva de tecnologías en la nube. A tres años de ese punto de inflexión, el Ministerio de Minas y Energía ha avanzado significativamente en la modernización de su infraestructura tecnológica y en la implementación de controles de seguridad alineados con estándares internacionales. Sin embargo, este mismo progreso ha expuesto nuevas superficies de riesgo y retos complejos en materia de gobernanza, riesgo y cumplimiento (GRC).

Durante 2025, el Ministerio consolidó un ecosistema tecnológico robusto mediante la implementación de herramientas de código abierto (Taiga, GitLab, GLPI, Nexus y Kubernetes), que han permitido modernizar los procesos de desarrollo, gestión de proyectos, soporte técnico y automatización de servicios. Estos avances representan un salto cualitativo en las capacidades operacionales del Grupo de Tecnologías de la Información y las Comunicaciones (GTIC). Paralelamente, se formalizó e implementó un Ciclo de Vida de Desarrollo Seguro (SDLC) que integra controles de seguridad desde las fases iniciales del desarrollo de software, con pipelines de integración continua y despliegue continuo (CI/CD) que automatizan validaciones de vulnerabilidades.

No obstante, los seguimientos trimestrales de 2025 también identificaron brechas críticas que requieren atención inmediata en 2026. La actualización del inventario de activos de información, aunque formalizada mediante la Circular 40028 en el tercer trimestre, no se completó según los cronogramas originales, revelando la complejidad de consolidar información en una organización descentralizada. Adicionalmente, el análisis de la auditoría interna puso de manifiesto la necesidad urgente de alinear completamente la matriz de activos con los nuevos lineamientos del Modelo de Seguridad y Privacidad de la Información

(MSPI) versión 3.0.2, particularmente en la identificación de infraestructura crítica cibernética conforme al Decreto 338 de 2022 y la Resolución 40646 de 2023.

Otro aspecto fundamental es la implementación de la herramienta de Gobernanza, Riesgo y Cumplimiento (GRC) dentro del sistema de información de SIGAME el cual hace seguimiento a los riesgos actuales de corrupción y fiscales. Esta herramienta será el cimiento para consolidar la visión integral de activos, riesgos, controles y responsabilidades, transformando la gestión manual y dispersa en un sistema centralizado, auditable y escalable que soporte la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

Durante 2025, el análisis de vulnerabilidades en sistemas de información identificó hallazgos de criticidad media y alta, principalmente vinculados a prácticas de desarrollo inseguro y ausencia de monitoreo centralizado de eventos de seguridad. Si bien el 85% de las vulnerabilidades altas y el 70% de las vulnerabilidades medias han sido remediadas, esta experiencia pone en evidencia que la madurez operativa del SDLC aún requiere consolidación y que la capacidad de detección y respuesta ante incidentes debe fortalecerse mediante soluciones de monitoreo centralizado.

Asimismo, el estado de implementación de controles mostró variaciones significativas: mientras algunos indicadores alcanzaron desempeño sobresaliente (100% de satisfacción en organización de seguridad y cobertura SGSI), otros descendieron a niveles críticos, como el indicador SGIN16 (implementación de controles) que alcanzó apenas el 40% en el tercer trimestre. Esta volatilidad refleja la necesidad de establecer mecanismos más robustos de seguimiento y aseguramiento en la implementación de actividades planificadas.

La gestión de activos de información constituye la brecha más significativa identificada. Sin una actualización completa desde 2021 en su clasificación y valoración, el Ministerio carece de insumos confiables para los Análisis de Impacto al Negocio (BIA) y Planes de Continuidad del Negocio (BCP), elementos críticos para la resiliencia organizacional y el cumplimiento del Decreto 338 en infraestructuras críticas.

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 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 Plan de Seguridad y Privacidad de la Información 2026 representa una evolución hacia la madurez operativa y la sostenibilidad de largo plazo. Los tres pilares estratégicos que guiarán este plan son:

1. **Consolidación e integración tecnológica**

   Completar la implementación de la plataforma GRC y consolidar el ecosistema DevOps, transformando procesos manuales y dispersos en flujos automatizados, auditables y escalables. Esta integración permitirá al GTIC generar visibilidad integral sobre activos, riesgos y controles, facilitando la toma de decisiones estratégicas basadas en datos confiables.

2. **Cierre de brechas críticas**

   Priorizar la actualización completa del inventario de activos de información, la alineación con el MSPI 2025 en infraestructura crítica cibernética, la generación de BIA y BCP actualizados, y la implementación de soluciones de monitoreo centralizado. Estos elementos son prerequisitos para cualquier avance adicional en madurez de seguridad.

3. **Resiliencia y continuidad operativa**

   Reforzar la capacidad del Ministerio para identificar, proteger, detectar, responder y recuperarse ante incidentes de seguridad, adoptando un enfoque basado en el NIST CSF y priorizando la continuidad del negocio en sectores críticos como el minero-energético.

4. ANTECEDENTES

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, 2025 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 2026. 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 2026 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:

5.1 Objetivo General

Consolidar la madurez operativa del Sistema de Gestión de Seguridad de la Información (SGSI) mediante la integración de gobernanza centralizada (GRC), la alineación completa con el Modelo de Seguridad y Privacidad de la Información (MSPI 2025), y la implementación de capacidades de identificación, detección, protección, respuesta y recuperación ante incidentes, garantizando la resiliencia de los sistemas de información del Ministerio de Minas y Energía y la continuidad de servicios críticos en el sector minero-energético.

5.2 Objetivos Específicos

1. Implementar y consolidar la plataforma de Gobernanza, Riesgo y Cumplimiento (GRC) como sistema centralizado de gestión de la seguridad de la información.
2. Actualizar completamente el Inventario de Activos de Información y alinearlo con los lineamientos del MSPI (2025), particularmente en la identificación de infraestructura crítica cibernética.
3. Generar y documentar Análisis de Impacto al Negocio (BIA) y Planes de Continuidad del Negocio (BCP) actualizados, alineados con MSPI y estrategia de resiliencia institucional.
4. Ejecutar la remediación completa de vulnerabilidades identificadas en sistemas de información y establecer un programa sostenible de gestión de vulnerabilidades.
5. Fortalecer la cultura organizacional de seguridad de la información mediante capacitación, sensibilización y comunicación continua.

6. ALCANCE

El Plan de Seguridad y Privacidad de la Información 2026 tiene como propósito fundamental garantizar la resiliencia de los sistemas de información del Ministerio, fortalecer la protección de activos digitales y críticos, y asegurar el cumplimiento normativo nacional e internacional. Este plan se desarrolla dentro del ciclo PHVA (Planificar, Hacer, Verificar, Actuar) y adopta una metodología de mejora continua que reconoce los avances de 2025 mientras aborda las brechas identificadas.

El alcance incluye todos los procesos, activos, personas y sistemas que intervienen en la gestión, uso y protección de la información institucional, extendiéndose a las dependencias internas del Ministerio, colaboradores, contratistas y terceros que gestionen datos relacionados con sus operaciones. La implementación de este plan se sustenta en controles administrativos, técnicos y operativos que garanticen la confidencialidad, integridad, disponibilidad 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

La gestión de activos de información es el cimiento del Sistema de Gestión de Seguridad de la Información (SGSI) del Ministerio de Minas y Energía. Sin una comprensión clara, actualizada y centralizada de qué activos posee la institución, sus características, criticidad y dependencias funcionales, es imposible implementar controles de seguridad efectivos, identificar y mitigar riesgos, o garantizar la continuidad operativa ante incidentes.

Esta sección describe el enfoque integral adaptado en 2026 para la identificación, clasificación, valoración y gestión de activos de información, alineado con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI 2025), el Decreto 338 de 2022 sobre Infraestructura Crítica Cibernética, la resolución 40646 de 2023, y los estándares internacionales ISO/IEC 27001:2022 e ISO/IEC 22301:2019.

De manera fundamental, esta sección integra tres actividades estrechamente relacionadas que deben ejecutarse de manera paralela y coordinada:

1. **Gestión de Activos de Información** - Identificación y clasificación
2. **Análisis de Impacto al Negocio (BIA)** - Determinación de criticidad funcional
3. **Planes de Continuidad del Negocio (BCP)** - Definición de estrategias de recuperación

Esta integración responde a la realidad operativa del Ministerio: no es posible desarrollar un BIA robusto sin conocer en detalle los activos que soportan cada proceso, ni es posible

crear planes de continuidad efectivos sin entender las dependencias críticas entre activos, procesos y objetivos estratégicos.

Tabla 1. *Actualización cronograma de actividades- Matriz de activos de información, BIA Y BCP.*

Actividad	Responsable	Fecha de Inicio	Fecha de Finalización	Descripción
Segunda fase capacitación sobre la matriz de activos	Equipo seguridad de la información	Segunda semana – Febrero 2026	Tercera semana - Febrero 2026	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	Tercera semana - Febrero 2026	Primera semana - Marzo 2026	Identificar y clasificar activos de información según los procesos de cada área
Segunda fase de revisión primaria de información enviada por las dependencias, definición de criticidad para ajustes de BIA.	Equipo seguridad de la información	Segunda semana - Marzo 2026	Tercera semana - Marzo 2026	Revisar documentación enviada por las dependencias (enlaces faltantes) , unificar información y establecer retroalimentación y mejora continua.
Ajustes y envío de retroalimentación a dependencias faltantes	Oficial de Seguridad o quien haga sus veces	Cuarta semana - Marzo 2026	Primera Semana - Abril 2026	En caso de presentarse información faltante o incompleta generar retroalimentación.
Entrega de información ajustada , ajustes de BIA y BCP	Responsables de cada dependencia	Segunda Semana - Abril 2026	Cuarta semana - Abril 2026	Información debidamente ajustada y completada.
Validación y priorización de activos críticos, entrega de BIA y BCP.	Oficial de Seguridad o quien haga sus veces	Cuarta semana - Abril 2026	Segunda semana - Mayo 2026	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 2026	Cuarta semana - Mayo 2026	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 representa el núcleo de la estrategia de seguridad del Ministerio de Minas y Energía. Durante el año 2025, el Grupo de Tecnologías de la Información y las Comunicaciones (GTIC) implementó de manera sistemática el Plan de Tratamiento de Riesgos, documentando avances significativos en la mitigación de vulnerabilidades críticas. Este plan para 2026 se construye sobre las lecciones aprendidas, reconociendo que la gestión de riesgos es un proceso dinámico y continuo que requiere ajuste permanente conforme evolucionan las amenazas y se fortalecen las capacidades institucionales.

El presente plan establece un marco integral que trasciende la simple implementación de controles técnicos, incorporando elementos de gobernanza, cultura organizacional, y alineación normativa. Se fundamenta en la metodología de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (Versión 6, DAFP), estándares internacionales como ISO/IEC 27001:2022, ISO/IEC 31000:2018 y NIST Cybersecurity Framework 2.0, así como en directrices nacionales incluidas en el Modelo de Seguridad y Privacidad de la Información (MSPI), Resolución 40646/2023 y Circular 40028/2025.

Durante 2025, la entidad avanzó en la identificación y clasificación de activos de información, implementó procedimientos estandarizados para auditoría de sistemas críticos, fortaleció la gestión de respaldos, y actualizó documentos esenciales como el BIA (Business Impact Analysis) y BCP (Business Continuity Plan). Sin embargo, el análisis de riesgos residuales evidenció que ciertos controles requieren profundización y que nuevas amenazas (particularmente en el contexto de infraestructura crítica y transformación digital) demandan una respuesta proactiva. El plan 2026 responde a estas necesidades con una estructura matricial de riesgos, diferenciados por criticidad e impacto operativo y de servicios, ya que, al no tener una matriz de activos consolidada, se dificultad mantener la metodología frente a la gestión basada en activos de información.

Tabla 2. *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 y privacidad de la información 2026	Equipo de seguridad de la información	Segunda semana - diciembre 2025	Tercera semana - diciembre 2025	A partir de las recomendaciones o hallazgos, ajustar actividades y procesos del plan de tratamiento de riesgos de seguridad y privacidad de la información.
Aprobación del plan de tratamiento de riesgos de seguridad y privacidad de la información	Oficina de planeación y gestión internacional (OPGI)	Segunda semana – enero 2026	Cuarta semana - enero 2026	Aprobación del plan de tratamiento de riesgos de seguridad y privacidad de la información.
Comunicación a las partes interesadas (controles a ejecutar)	Oficial de Seguridad o quien haga sus veces	Primera semana - febrero 2026	Segunda semana - febrero 2026	Según los controles (actividades) a realizar para la mitigación de los riesgos, se debe comunicar a las partes responsables los controles, seguimiento y la forma en la que deben reportar e implementar.
Desarrollo del plan de tratamiento de riesgos de seguridad y privacidad de la información	Equipo de seguridad de la información y partes interesadas	Primera semana - marzo 2026	Seguimiento trimestral	Seguimiento del plan y avance en la disminución de la probabilidad de materialización del riesgo.
Implementación de controles para los riesgos de seguridad y privacidad de la información	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 2026	Tercer trimestre año 2026	Evaluar la eficacia de las medidas implementadas y preparar un informe final.

Fuente grupo TICS

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 adaptará y adoptará la misma metodología de trabajo dispuesta desde el "E-ME-M-02 MANUAL DE GESTIÓN DE RIESGOS Y OPORTUNIDADES" que actualmente tiene la entidad.

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 3. *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 con los lineamientos de la norma ISO/IEC 27001:2022 adaptados a las necesidades y requerimientos del Ministerio.	Oficial de Seguridad o quien haga sus veces	Tercera semana - febrero 2026	Tercera semana - febrero 2026	Entrega de políticas, manuales, procedimientos, instructivos y protocolos, debidamente actualizados, ajustados o estructurados para primera revisión por parte del Grupo TICS.
Creación de nuevos documentos resultantes producto de la actividad anterior	Equipo e seguridad de la información	Primera semana - marzo 2026	Tercera semana - marzo 2026	Diseñar los documentos específicos para áreas críticas no cubiertas actualmente por el sistema de seguridad y privacidad de la información vigente.
Aprobación de los documentos resultantes.	Comité institucional de gestión y desempeño.	Segundo trimestre 2026	Segundo trimestre 2026	Validar y aprobar las políticas y procedimientos actualizados o nuevos.
Capacitación y sensibilización de los documentos aprobados.	Equipo de seguridad de la información	Primera semana - junio 2026	Cuarta semana - junio 2026	Socializar los cambios y formar a los responsables en su implementación.
Monitoreo de cumplimiento	Equipo de seguridad de la información	Seguimiento trimestral	Seguimiento trimestral	Seguimiento para verificar la adherencia y la efectividad de las políticas.
Revisión anual	Oficial de Seguridad o quien haga sus veces	Primera semana - diciembre 2026	Primera semana - diciembre 2026	Evaluar el estado general de las políticas y procedimientos para preparar el ciclo 2027.

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 2026 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 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 a continuación

Tabla 4. *Gestión de Recursos de Seguridad*

N°	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 - abril 2026
2	**Efectuar la revisión por la Alta Dirección**	Comité institucional de gestión y desempeño.	Tercera semana - abril 2026
3	**Generar informe de salidas de revisión por la Alta Dirección.**	Comité institucional de gestión y desempeño.	Cuarta semana - mayo 2026
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 - junio 2026
5	**Aprobación de presupuesto.**	Alta dirección	Cuarta semana - septiembre 2026

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

Tabla 5. *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 - febrero 2026	Primera semana - marzo 2026	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 – marzo 2026	Segunda semana - abril 2026	Establecimiento de líneas base para cada indicador clave.
Preparar el resultado de los indicadores para la revisión por la dirección.	**Oficial de Seguridad o quien haga sus veces**	Segunda semana - abril 2026	Cuarta semana - abril 2026	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 - mayo 2026	Segunda semana - mayo 2026	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 - mayo 2026	Cuarta semana - mayo 2026	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 a continuación.

Tabla 6. *Gestión de Vulnerabilidades Técnicas*

Actividad	Responsable	Fecha de Inicio	Fecha de Finalización	Descripción
Diseño del procedimiento e instrumentos	**Equipo de seguridad de la información**	Segunda semana - marzo 2026	Cuarta semana - marzo 2026	Crear y validar el formato estándar para la documentación de vulnerabilidades.
Capacitación en uso del formato	**Equipo de seguridad de la información**	Primera semana - abril 2026	Segunda semana - abril 2026	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 - abril 2026	Cuarta semana - abril 2026	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.

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 7. *Actividades llevadas a cabo en la ejecución de pruebas de pentesting*

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 27001:2022 y el Modelo de Seguridad y Privacidad de la información de MINTIC.

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 8. *Plan de Auditorias de Seguridad de la Información*

N°	Actividades	Responsable	Fecha
1	**Establecimiento del perfil del equipo auditor.**	Oficina de Control Interno	Primera semana- junio 2026
2	**Definición del grupo auditor.**	Oficina de Control Interno	Tercera semana - junio 2026
3	**Generar el listado de procesos a auditar con la fecha y hora en la que se realizará la auditoría**	Oficina de Control Interno	Primera semana - julio 2026
4	**Entrega de listado de información a entregar al auditor previa ejecución de la auditoría.**	Oficina de Control Interno	Segunda semana - julio 2026

N°	Actividades	Responsable	Fecha
5	**Reunión de Apertura de Auditoría**	Auditor	Segunda semana - agosto 2026
6	**Ejecución de auditoría.**	Auditor	Tercera semana- Cuarta semana - agosto 2026
7	**Reunión de Cierre de auditoría**	Auditor	Cuarta semana - septiembre 2026
8	**Redacción de informe de auditoría**	Auditor	Segunda semana - septiembre 2026
9	**Presentación de informe de auditoría**	Auditor	Tercera semana - septiembre 2026
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 - octubre 2026

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 9. *Mejoramiento Continuo*

N°	Actividades	Responsable	Fecha
1	**Planeación de cierre de brechas de las auditorias 2025**	Oficial de seguridad de la información o quien haga sus veces.	Marzo 2026
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 - marzo 2026
3	**Ejecutar las acciones para controlar y corregir las no conformidades.**	Oficial de seguridad de la información o quien haga sus veces.	Tercera semana - marzo 2026
5	**Revisar la eficacia de las acciones correctivas tomadas.**	Oficial de seguridad de la información o quien haga sus veces.	Tercera semana - junio 2026
6	**Realizar los cambios al SGSI de ser necesario.**	Oficial de seguridad de la información o quien haga sus veces.	Tercera semana – agosto 2026

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.

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 10. *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. - Primarios.	Reportes ejecutivos, decisiones estratégicas.	Mensual.
Comité Institucional de Gestión y Desempeño	Grupo encargado de implementar y desarrollar las políticas de	- Internos.	Políticas de gestión, actualizaciones normativas.	Trimestral.

Grupo de Interés	Descripción	Características	Necesidades Clave	Frecuencia de Comunicación
	gestión del MIPG, según el Decreto 1499 de 2017.	- Primarios.		
Colaboradores de TI	Colaboradores que trabajan en la Gerencia de Tecnologías de la Información.	- Internos y externos. - Primarios y secundarios.	Capacitación en políticas y procedimientos.	Según necesidad.
Oficina de planeación y gestión organizacional	Colaboradores de la Gerencia de Planeación Institucional.	- Internos y externos. - Primarios y secundarios.	Directrices para la alineación estratégica.	Mensual.
Oficina de Control Interno	Personal de la Oficina de Control Interno.	- Internos. - Primarios.	Reportes de cumplimiento, auditorías.	Trimestral.
Ciudadanos	Ciudadanos de Colombia que interactúan con los servicios del Ministerio.	- Externos. - Secundarios.	Transparencia en políticas y seguridad.	Anual o según eventos.
Todos los colaboradores del MINENERGÍA	Funcionarios y contratistas del Ministerio de Minas y Energía.	- Internos y externos. - Primarios y secundarios.	Sensibilización, cumplimiento de políticas.	Trimestral.
Secretaría General	La(o) secretaria(o) general del MINENERGÍA.	- Internos. - Primarios.	Información estratégica y de alto nivel.	Mensual.

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 **caracterización**).
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.

Tabla 11. *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, 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.

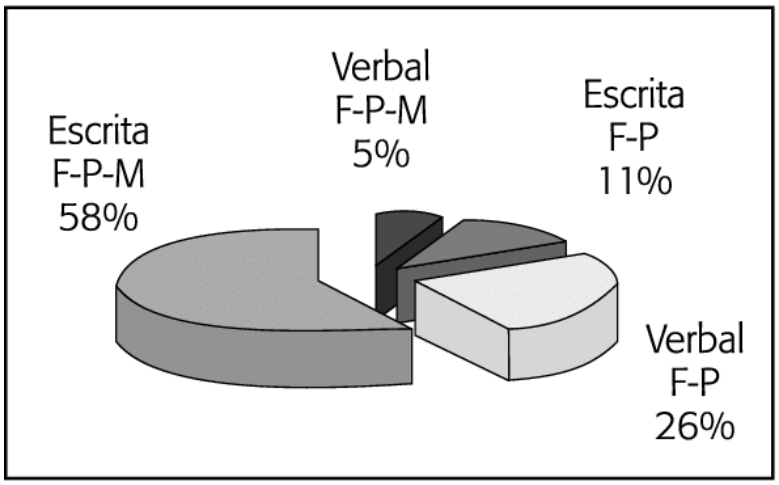
7.4.1 Sensibilización

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

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:

1. **E-card:** Consiste en diseñar una tarjeta virtual llamativa, con poco texto y más imágenes, esta modalidad es más efectiva a la hora de trasmitir mensajes muy puntuales y concisos.
2. **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.
3. **Videos animados:** Consiste en diseñar presentaciones animadas y videos explicativos animados muy cortos de máximo de 5 minutos de duración.
4. **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.
5. **Cartillas**: es una revista corta de un tema específico, cuyo propósito es orientar sobre un tema de interés.

6. **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.
7. **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.
8. **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.

1. **Correo**: Se trata del correo institucional en Microsoft Teams con dominio minienergia.gov.co establecido por la Entidad para todos los comunicados oficiales.

2. **Portal web:** Se trata de la página web oficial: https://www.minenergía.gov.co/ de la Entidad.

3. 

4. **Pantallas**: Se trata de pantallas ubicadas en diferentes sitios estratégicos de la Entidad para su consulta en sitio.

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:

1. Ministro y directores.
2. Jefes de oficina y coordinadores.
3. Líderes de proceso.
4. Comité institucional de gestión y desempeño.
5. Oficial de seguridad de la información.
6. Profesionales de seguridad de la información.
7. Grupo de soporte informático.
8. Propietarios de la información.
9. 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:

1. **Presencial**: Catedra dirigida en las instalaciones de la Entidad.
2. **Virtual**: Catedra dirigida y realizada por medio de herramientas virtuales de comunicación como lo son *Google meet, Microsoft teams*, entre otros.
3. **Estudio autónomo**: Consiste en sesiones organizadas por módulos con objetos virtuales de aprendizaje que son parte de un proceso de estudio asincrónico, es decir son previamente 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 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 12. *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, Equipo seguridad de la información	Primera semana – junio 2026	Segunda semana - junio 2026	Determinar el tipo de incidente a simular (e.g., ciberataque, filtración de datos). Definir el impacto y las áreas involucradas.
Desarrollo de los procedimientos del ejercicio	Oficial de Seguridad o quien haga sus veces, Equipo seguridad de la información	Tercera semana - junio 2026	Cuarta semana - junio 2026	Elaborar los protocolos y guías de respuesta, los roles de los participantes y los resultados esperados del ejercicio.
Planificación de la logística	Grupo TICS	Tercera semana – Julio 2026	Cuarta semana - Julio 2026	Organizar los recursos necesarios para el ejercicio (infraestructura, equipos, acceso).
Simulación del ejercicio	Oficial de Seguridad o quien haga sus veces, Grupo TICS	Segunda semana – septiembre 2026	Tercera semana – septiembre 2026	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 plan de actualización de políticas y procedimientos	Oficial de Seguridad o quien haga sus veces /Seguridad de la información	Segunda semana - septiembre 2026	Segunda semana - diciembre 2026	Revisar y ajustar las políticas y procedimientos de seguridad en función de los resultados del ejercicio.

Fuente grupo TICS

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 13. *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.

Categoría	Tema	Descripción
	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.
	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.

Categoría	Tema	Descripción
	Integridad en la cadena de suministro digital	Gestión de riesgos con proveedores y terceros que manejan información del Ministerio.
	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

1. Desarrollar y mantener actualizadas las políticas y procedimientos de seguridad, asegurando su alineación con las normativas nacionales e internacionales aplicables.
2. Incluir lineamientos específicos para la protección de infraestructuras críticas y sistemas específicos del sector energético y minero.
3. Implementar programas regulares de capacitación para todos los niveles de la organización, desde la Alta Dirección hasta el personal operativo.
4. Adaptar los temas de capacitación a riesgos emergentes y actualizaciones normativas.
5. Realizar evaluaciones periódicas de riesgos en los sistemas de información y activos críticos.
6. Priorizar la implementación de controles sobre los riesgos identificados como de mayor criticidad.
7. Establecer un proceso estructurado para la identificación, análisis, respuesta y recuperación ante incidentes de seguridad.
8. Simular escenarios de crisis para evaluar la efectividad de los planes de respuesta.
9. Implementar herramientas de monitoreo para identificar amenazas en tiempo real y prevenir incidentes.
10. 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 27000:2022)

- **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 27000:2022)

- **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 27000:2022)

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

- **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 27000:2022)

- **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 27000:2022)

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. **Estrategia Nacional de Seguridad Digital 2025-2027**
2. **Modelo de Seguridad y Privacidad de la Información 2025 (MSPI)**: Estándar colombiano para la gestión de la seguridad y privacidad en las entidades públicas.
3. **Resolución 40646 de 2023 (MINENERGÍA)**: Define el marco de las políticas de seguridad de la información para el Ministerio de Minas y Energía.
4. **Ley 1581 de 2012**: Régimen general de protección de datos personales en Colombia.
5. **Guía DAFP**: Guía Administración del Riesgo y el diseño de controles en entidades públicas, emitida por el Departamento Administrativo de la Función Pública.