Manual de Políticas del Sistema de Gestión de Seguridad de la Información - MPSGSI

**2024**

VERSIÓN EN REVISIÓN

FECHA 20/12/2024

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

# LISTADO DE VERSIONES

**Tabla 1**  
Listado de Versiones

|  |  |  |
| --- | --- | --- |
| VER. | FECHA | RAZÓN DE LA ACTUALIZACIÓN |
| 1.0 | 17/02/2022 | Versión inicial del documento |
| 2.0 | 20/12/2024 | Actualización para vigencia 2025 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Fuente: MINENERGÍA

# APROBACIONES

**Tabla 2**   
Aprobaciones

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ELABORÓ | | REVISÓ | | APROBÓ | |
| Cargo: | Andrés Camilo Molano - Encargado seguridad de la información | Cargo: | Profesional Especializado | Cargo: |  |
| Dependencia: | GRUPO TICS | Dependencia: | Grupo TICS | Dependencia: | OPGI |
| Fecha: | 20/12/2024 | Fecha: |  | Fecha: |  |

Fuente: MINENERGÍA

INDICE DE CONTENIDO

[LISTADO DE VERSIONES 2](#_Toc186458192)

[APROBACIONES 2](#_Toc186458193)

[1. INTRODUCCIÓN 5](#_Toc186458194)

[2. JUSTIFICACIÓN 6](#_Toc186458195)

[3. CONTEXTUALIZACIÓN 7](#_Toc186458196)

[4. ANTECEDENTES 7](#_Toc186458197)

[5. OBJETIVOS 8](#_Toc186458198)

[5.1 OBJETIVO GENERAL 8](#_Toc186458199)

[5.2 OBJETIVOS ESPECÍFICOS 8](#_Toc186458200)

[6. ALCANCE 9](#_Toc186458201)

[7. Manual de Políticas del SGSI 9](#_Toc186458202)

[7.1 Políticas mandatarías o requisitos ISO 27001 9](#_Toc186458203)

[7.1.1 Política general de Seguridad y Privacidad de la Información 9](#_Toc186458204)

[7.1.2 Política de tratamiento y protección de datos personales 13](#_Toc186458205)

[7.1.3 Política de continuidad del negocio o del sistema de gestión y continuidad del negocio (SGCN) 17](#_Toc186458206)

[7.1.4 Política de Recuperación ante Desastres TIC 20](#_Toc186458207)

[7.2 Políticas de seguridad y privacidad de la información 24](#_Toc186458208)

[7.2.1 Política para gestión de riesgos de Seguridad de la Información 24](#_Toc186458209)

[7.2.2 Política de separación de deberes 25](#_Toc186458210)

[7.2.3 Política de contacto con autoridades de seguridad de la información 27](#_Toc186458211)

[7.2.3 Política de gestión de grupos de interés especial 30](#_Toc186458212)

[7.2.4 Política de Seguridad de la Información en la Gestión de Proyectos 31](#_Toc186458213)

[7.2.5 Política de dispositivos móviles 33](#_Toc186458214)

[7.2.6 Política BYOD (Bring Your Own Device) 35](#_Toc186458215)

[7.2.8 Política de gestión humana 39](#_Toc186458216)

[7.2.9 Política de gestión y uso aceptable de activos 42](#_Toc186458217)

[7.2.10 Política de uso aceptable de activos de información 45](#_Toc186458218)

[7.2.11 Política para clasificación de la información 47](#_Toc186458219)

[7.2.12 Política de control de acceso 50](#_Toc186458220)

[7.2.13 Política para gestión de autenticación secreta de usuarios o de contraseñas 53](#_Toc186458221)

[7.2.14 Política para uso de controles criptográficos 55](#_Toc186458222)

[7.2.15 Política para gestión de llaves criptográficas 60](#_Toc186458223)

[7.2.16 Política de seguridad física y trabajo en áreas seguras 62](#_Toc186458224)

[7.2.17 Política de escritorio y pantalla limpia 66](#_Toc186458225)

[7.2.18 Política para control de cambios 69](#_Toc186458226)

[7.2.19 Política de protección contra códigos maliciosos 73](#_Toc186458227)

[7.2.20 Política de respaldo de información 75](#_Toc186458228)

[7.2.21 Política de registro de eventos 78](#_Toc186458229)

[7.2.23 Política de restricciones sobre la instalación de software 84](#_Toc186458230)

[7.2.24 Política sobre auditorías de sistemas de información 86](#_Toc186458231)

[7.2.25 Política de gestión de la seguridad de las redes 88](#_Toc186458232)

[7.2.26 Política de transferencia de información y cifrado 91](#_Toc186458233)

[7.2.27 Política de uso de correo electrónico 94](#_Toc186458234)

[7.2.28 Política para adquisición, desarrollo y mantenimiento seguro de software 97](#_Toc186458235)

[7.2.29 Política de relaciones con proveedores 100](#_Toc186458236)

[7.2.31 Políticas de cumplimiento 105](#_Toc186458237)

[7.2.32 Política de eliminación y destrucción segura de información 108](#_Toc186458238)

[8. GLOSARIO 111](#_Toc186458239)

[9. REFERENCIAS 114](#_Toc186458240)

# INTRODUCCIÓN

En un entorno donde la tecnología y la digitalización son fundamentales para el desarrollo de los sectores estratégicos, la seguridad de la información se ha convertido en un pilar esencial para garantizar la continuidad operativa, la confianza de los ciudadanos y el cumplimiento de los objetivos institucionales. En el caso del Ministerio de Minas y Energía, la protección de los activos de información es crítica, ya que sustenta la toma de decisiones en la gestión de los recursos energéticos y minerales del país.

El Sistema de Gestión de Seguridad de la Información (SGSI) del Ministerio está diseñado para abordar estos retos, proporcionando un marco que identifica, gestiona y protege los activos de información frente a amenazas internas y externas. Este manual, actualizado con los lineamientos de la Resolución 40646 y los estándares internacionales, como la ISO/IEC 27001:2022, establece las políticas que rigen la seguridad de la información y refuerzan la capacidad del Ministerio para adaptarse a un entorno dinámico y en constante evolución.

La actualización de este manual responde a la necesidad de garantizar que las políticas reflejen las mejores prácticas internacionales y respondan a las amenazas emergentes, como los ciberataques dirigidos a infraestructuras críticas. Además, destaca el compromiso del Ministerio con la confidencialidad, integridad y disponibilidad de la información, así como con la promoción de una cultura organizacional que priorice la seguridad digital en todos los niveles.

Este documento se presenta como una herramienta estratégica que articula los objetivos del SGSI con los requerimientos legales, técnicos y operativos del Ministerio. Su aplicación abarca todos los procesos y áreas funcionales, promoviendo una gestión de riesgos proactiva que permite identificar vulnerabilidades, implementar controles efectivos y garantizar la resiliencia frente a incidentes.

En definitiva, este manual no solo guía la implementación y mantenimiento del SGSI, sino que también refuerza el rol del Ministerio de Minas y Energía como un referente en la seguridad de la información dentro del sector público. Al adoptar estas políticas, se asegura el cumplimiento de las metas institucionales, el desarrollo sostenible del sector energético y la confianza de la sociedad en el manejo responsable de los recursos de información.

# JUSTIFICACIÓN

El Sistema de Gestión de Seguridad de la Información (SGSI) es un pilar esencial en la estrategia del Ministerio de Minas y Energía, ya que garantiza la protección de los activos de información que soportan sus operaciones estratégicas y misionales. En un entorno cada vez más digitalizado y vulnerable a amenazas cibernéticas, este manual se convierte en una herramienta indispensable para establecer un marco de políticas y directrices que aseguren la confidencialidad, integridad y disponibilidad de la información en todos los niveles de la organización.

La actualización del manual responde a las demandas actuales de seguridad digital, alineándose con los lineamientos de la Resolución 40646 y estándares internacionales como la ISO/IEC 27001:2022, que promueven un enfoque sistemático y proactivo en la gestión de riesgos de seguridad de la información. Esta justificación también contempla la necesidad de cumplir con las normativas regulatorias y fortalecer la resiliencia cibernética frente a incidentes que puedan comprometer la continuidad operativa y la confianza pública.

El Ministerio, como ente rector del sector energético y minero, maneja información crítica para la toma de decisiones estratégicas, así como datos sensibles de ciudadanos, empresas y recursos nacionales. Esto subraya la importancia de contar con políticas actualizadas que mitiguen riesgos asociados a ciberataques, pérdida de datos, o accesos no autorizados, protegiendo tanto la infraestructura tecnológica como la reputación institucional.

Este documento también tiene como objetivo fomentar una cultura organizacional basada en la seguridad de la información, involucrando a todos los niveles de la entidad en el cumplimiento de las políticas y medidas preventivas. Esto no solo garantiza la efectividad del SGSI, sino que también posiciona al Ministerio como un modelo de buenas prácticas en seguridad de la información dentro del sector público.

En última instancia, la actualización de este manual es una inversión estratégica para garantizar que el Ministerio pueda cumplir con sus objetivos institucionales de manera eficiente, segura y transparente, respondiendo a los desafíos tecnológicos y regulatorios del presente y del futuro.

# CONTEXTUALIZACIÓN

El Ministerio de Minas y Energía desempeña un rol estratégico en la gestión y administración de los recursos energéticos y minerales de Colombia, sectores que son fundamentales para el desarrollo económico y social del país. En este contexto, el manejo adecuado de la información es clave para garantizar la continuidad operativa, la confianza de las partes interesadas y el cumplimiento de los objetivos institucionales.

Con la creciente digitalización de los procesos y la adopción de tecnologías emergentes, el Ministerio enfrenta retos significativos en términos de seguridad de la información. Las amenazas cibernéticas, como el robo de datos, los ataques a infraestructuras críticas y la proliferación de ransomware, exigen la implementación de medidas de seguridad integrales y una gestión proactiva de los riesgos digitales.

Esta sección contextualiza la importancia del SGSI en un entorno dinámico donde la información no solo es un activo estratégico, sino también un objetivo constante de actores malintencionados. Además, subraya el compromiso del Ministerio de adoptar políticas que alineen la seguridad de la información con los objetivos institucionales y el marco regulatorio nacional, promoviendo una cultura de ciberseguridad y resiliencia digital.

# ANTECEDENTES

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

Durante el año 2024, el Ministerio desarrolló un marco robusto de gestión de riesgos, que facilitó el registro y control de actividades críticas como la identificación de activos (matriz desarrollada), la evaluación de riesgos en desarrollo y el manejo de incidentes (procedimientos). Estas acciones permitieron una mayor visibilidad sobre las vulnerabilidades de la entidad, impulsando la implementación de controles correctivos y la priorización de activos críticos (procesos actuales). Además, las auditorías internas y externas realizadas evidenciaron la necesidad de ajustes en los procedimientos para responder con mayor agilidad a las amenazas emergentes.

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

# OBJETIVOS

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

## 5.1 OBJETIVO GENERAL

Fortalecer la seguridad y privacidad de la información del Ministerio de Minas y Energía, mediante la adopción de políticas, controles y lineamientos alineados al Modelo de Seguridad y Privacidad de la Información (MSPI) y las normas ISO/IEC 27001:2022 e ISO/IEC 22301:2019, promoviendo una cultura organizacional de ciberseguridad y asegurando la continuidad del negocio y el cumplimiento normativo.

## 5.2 OBJETIVOS ESPECÍFICOS

1. Establecer un marco robusto de gestión de riesgos de seguridad de la información y ciberseguridad, identificando y mitigando las vulnerabilidades que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información, conforme a las directrices de la norma ISO/IEC 27001:2022 y los principios del MSPI​

​

1. Promover la resiliencia operativa y la continuidad del negocio, implementando y manteniendo políticas que aseguren la capacidad de respuesta ante incidentes y desastres, alineadas con los requerimientos de la norma ISO/IEC 22301:2019 y los planes de continuidad del MSPI​

​

1. Fomentar una cultura institucional de seguridad digital, mediante la sensibilización, capacitación y asignación de responsabilidades claras a todos los colaboradores y partes interesadas del Ministerio, para garantizar el cumplimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) y los lineamientos establecidos por el Ministerio de Minas y Energía.

​

.

# ALCANCE

El presente documento establece las políticas del Sistema de Gestión de Seguridad de la Información (SGSI) del Ministerio de Minas y Energía, en alineación con los estándares internacionales ISO 27001:2022 e ISO 27002:2022, así como con las disposiciones del Modelo de Seguridad y Privacidad de la Información (MSPI). Estas políticas están diseñadas para ser aplicadas a los procesos estratégicos, misionales, de apoyo, evaluación, control y especiales del Ministerio, y a todos los activos de información, repositorios y sistemas tecnológicos que soportan su operación.

El alcance incluye a todas las partes interesadas, internas y externas, que interactúan con la información del Ministerio, ya sea que la gestionen, almacenen o accedan a ella mediante medios físicos o digitales. También contempla la protección de la infraestructura energética crítica y las operaciones relacionadas con la continuidad del negocio, incorporando avances tecnológicos como soluciones en la nube, dispositivos móviles y sistemas inteligentes

En cumplimiento de estas políticas, se busca garantizar la confidencialidad, integridad y disponibilidad de la información, apoyando las funciones críticas del Ministerio en un entorno seguro y resiliente. Este alcance será revisado anualmente o siempre que surjan cambios significativos en el marco normativo, en los procesos del SGSI, o en los objetivos estratégicos de la Entidad.

# Manual de Políticas del SGSI

A continuación, se relacionan cada una de las políticas a tratar dentro de este documento:

## 7.1 Políticas mandatarías o requisitos ISO 27001

Este capítulo establece las políticas mínimas que solicita la norma ISO 27001:2022 y que son exigibles en procesos de auditoría. Se definen y publican, además, como parte integral de la resolución del MINENERGÍA.

### Política general de Seguridad y Privacidad de la Información

El principal objetivo de esta política es establecer un marco robusto de lineamientos que permita proteger los activos de información del Ministerio de Minas y Energía frente a riesgos que puedan comprometer su confidencialidad, integridad y disponibilidad. A través de esta política, se busca garantizar que toda la información procesada, almacenada y transmitida por el Ministerio esté adecuadamente protegida contra amenazas internas y externas, fortaleciendo la confianza de las partes interesadas y promoviendo el cumplimiento de los requisitos normativos y regulatorios aplicables.

Además, esta política tiene como propósito alinear las acciones de la Entidad con los estándares internacionales en seguridad de la información, como la NTC-ISO 27001:2022, y con el Modelo de Seguridad y Privacidad de la Información (MSPI). Este enfoque asegura que los riesgos asociados con los procesos críticos del Ministerio sean identificados, evaluados y gestionados eficazmente, integrando la seguridad de la información en las actividades misionales, estratégicas y de apoyo. También fomenta una cultura organizacional centrada en la prevención de incidentes, la gestión proactiva de vulnerabilidades y la continuidad operativa frente a eventos adversos.

Finalmente, esta política establece el compromiso del Ministerio de fortalecer la capacidad institucional para enfrentar los desafíos de un entorno digital dinámico y cada vez más interconectado. Se enfatiza la importancia de gestionar los riesgos de seguridad de manera integral, asegurando que todas las partes interesadas, incluyendo funcionarios, contratistas y la ciudadanía, comprendan su papel en la preservación de la seguridad y privacidad de la información. Este objetivo se apoya en el desarrollo continuo de competencias, la implementación de controles tecnológicos avanzados y la promoción de buenas prácticas en el manejo responsable de la información.

**Principios de Seguridad de la Información:**

* **Definir, implementar y mejorar el SGSI:** Asegurar un ciclo continuo de mejora en el sistema de gestión de seguridad de la información, alineado con las necesidades estratégicas de la Entidad y los marcos regulatorios.
* **Responsabilidad compartida:** Todos los usuarios, internos y externos, deben asumir responsabilidades específicas relacionadas con la seguridad y privacidad de la información.
* **Protección de la información crítica:** Preservar la confidencialidad, integridad y disponibilidad de los activos de información asociados a procesos críticos del negocio.
* **Aplicación de controles según clasificación:** Implementar medidas de protección basadas en la clasificación de la información, minimizando impactos financieros, operativos y legales.
* **Mitigación de riesgos internos:** Proteger la información contra amenazas originadas por el personal interno mediante controles específicos y formación.
* **Seguridad en infraestructura tecnológica:** Garantizar que las instalaciones físicas y tecnológicas cumplan con estándares de seguridad que respalden los procesos críticos del Ministerio.
* **Control de operaciones críticas:** Supervisar y garantizar la seguridad en las operaciones de negocio, incluyendo recursos tecnológicos y redes.
* **Gestión de acceso restringido:** Establecer controles estrictos para el acceso a sistemas, información y recursos de red, basados en el principio de privilegio mínimo.
* **Integración de la seguridad en el ciclo de vida:** Incorporar controles de seguridad en todas las fases del desarrollo y mantenimiento de sistemas de información.
* **Gestión proactiva de incidentes y vulnerabilidades:** Mejorar continuamente la seguridad mediante la detección, análisis y mitigación de eventos e incidentes relacionados con la información.
* **Continuidad del negocio:** Asegurar la disponibilidad de los procesos críticos del negocio ante eventos disruptivos, mediante planes sólidos de continuidad y recuperación.
* **Cumplimiento normativo:** Garantizar que las actividades de la Entidad cumplan con las obligaciones legales, regulatorias y contractuales, promoviendo la transparencia y la rendición de cuentas.

En concordancia con la política global de seguridad de la Información, se establecen:

* **Objetivos anuales de seguridad:** Definir objetivos alineados con los riesgos y las prioridades estratégicas del Ministerio.
* **Metodología de gestión de riesgos:** Implementar una metodología estructurada para identificar, evaluar y tratar riesgos relacionados con la información.
* **Controles de seguridad efectivos:** Diseñar e implementar controles adecuados que mitiguen los riesgos identificados y respalden el plan de tratamiento.
* **Cumplimiento de requisitos legales y contractuales:** Asegurar que todas las actividades de la Entidad cumplan con las normativas aplicables.
* **Medios para la continuidad operativa:** Establecer recursos y capacidades necesarias para garantizar la continuidad de las operaciones ante eventos adversos.
* **Sanciones por incumplimiento:** Aplicar medidas disciplinarias para violaciones a esta política o cualquier procedimiento del SGSI.
* **Reporte obligatorio de incidentes:** Asegurar que todo funcionario informe sobre violaciones, confirmadas o sospechadas, de la seguridad de la información.
* **Asignación de responsabilidades:** Establecer claramente las responsabilidades de los funcionarios y el Oficial de Seguridad de la Información para la implementación, mantenimiento y supervisión de esta política.

**Alcance/Aplicabilidad**

Esta política es aplicable a todos los procesos estratégicos, misionales, de apoyo, evaluación y control del Ministerio de Minas y Energía, así como a sus recursos tecnológicos, información y datos gestionados en cualquier medio. Incluye a los usuarios internos y externos, colaboradores, contratistas, proveedores, y cualquier persona o entidad que acceda, procese, almacene o transmita información perteneciente al Ministerio.

La política también se extiende a la infraestructura tecnológica, tanto física como digital, que soporta las operaciones del Ministerio, incluyendo sistemas en la nube, redes, dispositivos móviles y equipos críticos. Asimismo, involucra a la ciudadanía en general que interactúe con los servicios ofrecidos por la Entidad, garantizando la protección y el manejo adecuado de la información personal y pública.

**Nivel de Cumplimiento de la Política**

Todas las personas y entidades cubiertas por el alcance de esta política están obligadas a cumplir plenamente con sus disposiciones, sin excepción. El cumplimiento del 100% de esta política es esencial para preservar la confidencialidad, integridad y disponibilidad de los activos de información, así como para mantener la confianza de las partes interesadas.

El Ministerio realizará auditorías periódicas y monitoreos continuos para verificar la adherencia a esta política. Cualquier incumplimiento será tratado de acuerdo con los procedimientos disciplinarios establecidos, incluyendo posibles sanciones administrativas o legales en caso de violaciones graves.

**Excepciones a la Política**

Cualquier excepción o modificación a esta política deberá ser previamente justificada, documentada y aprobada por el Oficial de Seguridad de la Información o por quien haga sus veces. Estas excepciones serán revisadas y validadas por la Mesa de Trabajo de Seguridad y Privacidad de la Información y Continuidad del Negocio, garantizando que no comprometan los principios fundamentales de la seguridad de la información del Ministerio.

Las solicitudes de excepción deberán incluir una evaluación detallada de riesgos y las medidas de mitigación que se implementarán para minimizar posibles impactos negativos.

**Revisiones**

Esta política será objeto de revisiones periódicas, al menos una vez al año, para garantizar su alineación con las necesidades del Ministerio, los cambios regulatorios, tecnológicos y organizacionales, y las mejores prácticas en seguridad de la información.

Además, las revisiones se llevarán a cabo cada vez que ocurra un cambio significativo en los componentes del SGSI, del Sistema de Gestión de Continuidad del Negocio (SGCN), del Modelo de Seguridad y Privacidad de la Información (MSPI), o en las necesidades y expectativas de las partes interesadas. Las actualizaciones serán comunicadas de manera efectiva a todos los usuarios y colaboradores relevantes para asegurar su comprensión y aplicación.

### 7.1.2 Política de tratamiento y protección de datos personales

**Objetivo de la Política:**

El objetivo de esta política es garantizar el tratamiento adecuado y seguro de los datos personales recolectados, almacenados, utilizados, transmitidos o eliminados por el Ministerio de Minas y Energía, en cumplimiento de la Ley Estatutaria 1581 de 2012, el Decreto 1377 de 2013, y demás normativas aplicables. Se busca proteger la autenticidad, confidencialidad, integridad y disponibilidad de los datos personales, respetando los derechos fundamentales de los titulares, incluidos el habeas data y la privacidad, a través de controles adecuados y buenas prácticas.

**Ámbito de Aplicación**

Esta política aplica a todas las áreas y procesos del Ministerio, incluidos funcionarios, contratistas, aliados estratégicos y cualquier persona o entidad que acceda o trate datos personales bajo la responsabilidad del Ministerio. Abarca todos los sistemas y bases de datos, tanto en medios físicos como electrónicos, que contengan información de personas naturales.

El Ministerio de Minas y Energía , establece un “Compromiso de Confidencialidad”, el cual deberá ser suscrito por todos los funcionarios, en el cual se comprometen a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del responsable de los datos de que se trate.

En ese contexto, el Ministerio de Minas y Energía, reconociendo que el habeas data o protección de datos personales es una extensión del derecho a la intimidad, que los principios para el establecimiento de la política de tratamiento de datos personales a cumplir por la entidad son:

1. **Principio de la Legalidad:** El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente. El tratamiento de datos personales es una actividad regulada que debe sujetarse a lo establecido en la Ley y en las demás disposiciones que la desarrollen.
2. **Principio de finalidad:** Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular. El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley.
3. **Principio de libertad:** El tratamiento solo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
4. **Principio de veracidad o calidad**: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
5. **Principio de transparencia:** Garantizar al titular de los datos, el derecho a obtener información que le concierna del encargado del tratamiento. En el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
6. **Principio de acceso y circulación restringida:** El tratamiento solo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente. El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de ley y la Constitución. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la ley; Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados.
7. **Principio de seguridad:** La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas, que sean necesarias para garantizar la seguridad, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
8. **Principio de confidencialidad:** Todas las personas que participen en el Tratamiento de Datos Personales, deben garantizar la reserva y confidencialidad de dicha información. Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos, están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

**Derechos de los titulares**

El tratamiento específico para cada base de datos personales debe ser definido, autorizado previamente, registrado y comunicado al titular de la información. El Ministerio de Minas y Energía implementa de manera permanente las acciones necesarias para dar efectividad al derecho consagrado en la Ley Estatutaria 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por lo que da a conocer a todos sus ciudadanos-clientes los derechos que se derivan de la protección de datos personales y que se relacionan a continuación:

1. Conocer, actualizar y rectificar sus datos personales. Conocer, actualizar y rectificar su información frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté prohibido o no haya sido autorizado
2. Solicitar la prueba de su autorización para el tratamiento de sus datos personales, salvo en los casos establecidos en el artículo 10 de la Ley 1581 de 2012.
3. Ser informado respecto del uso que se les da a sus datos personales, previa solicitud.
4. Revocar la autorización y/o solicitar la supresión de sus datos personales de las bases de datos o archivos cuando el titular lo considere, siempre y cuando no se encuentren vigentes con la Entidad los servicios o productos que dieron origen a dicha autorización.
5. Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.
6. Presentar quejas ante la Entidad administrativa encargada de la protección de los datos personales. Presentar ante la Superintendencia de Industria y Comercio (SIC), quejas por las infracciones a lo dispuesto en la normatividad vigente.
7. El tratamiento de datos personales de niños, niñas y adolescentes está prohibido en la Entidad, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7 de la Ley 1581 de 2012 y el artículo 12 del Decreto 1377 de 2013.
8. Al realizar uso de alguna de las aplicaciones móviles del Ministerio de Minas y Energía, se estará recolectando información de los tipos de usuarios que acceden, ubicación (ciudad) y tipos de dispositivos móviles.

El incumplimiento a la política de Seguridad y Privacidad de la Información del Ministerio de Minas y Energía, traerá consigo las consecuencias legales, según la normativa de la Entidad y las normas que competen al Gobierno Nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere sin excepción.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, los usuarios y colaboradores de la entidad, incluyendo contratistas, proveedores y terceros que, de alguna manera, tengan acceso a información o datos personales bajo la custodia de la Entidad. Asimismo, incluye a la ciudadanía en general, como titulares de los datos personales que son tratados por el Ministerio de Minas y Energía en el ejercicio de sus funciones.

Además, esta política es aplicable a todos los sistemas de información, procesos, activos tecnológicos y canales de comunicación utilizados para el tratamiento de datos personales, ya sea en formato físico o digital, dentro y fuera de las instalaciones de la Entidad.

**Nivel de Cumplimiento de la Política**

Todas las personas cubiertas por el alcance y aplicabilidad de esta política deben cumplir en su totalidad con las directrices aquí establecidas. El cumplimiento debe ser verificado regularmente mediante auditorías internas y mecanismos de seguimiento establecidos en el marco del Sistema de Gestión de Seguridad de la Información (SGSI).

El incumplimiento de esta política podrá acarrear medidas correctivas, sanciones administrativas, y, de ser necesario, acciones legales, conforme a las normativas vigentes aplicables al sector público y a la protección de datos personales.

**Excepciones a la política**

Cualquier excepción o desviación a la presente política deberá ser justificada de manera documentada, aprobada por el Oficial de Seguridad de la Información y/o quien haga sus veces, y revisada en las Mesas de Trabajo de Seguridad y Privacidad de la Información y Continuidad del Negocio. Las excepciones se registrarán y documentarán para su seguimiento, y se deberán definir medidas compensatorias para mitigar riesgos asociados.

**Revisiones**

Esta política será revisada al menos una vez al año, considerando los resultados de auditorías internas, cambios regulatorios, incidentes de seguridad relevantes, y retroalimentación de las partes interesadas.

Adicionalmente, las revisiones deberán contemplar:

* Cambios normativos en materia de protección de datos personales a nivel nacional e internacional.
* Actualizaciones en el MSPI, el SGSI o el SGCN que afecten directa o indirectamente los procedimientos asociados al tratamiento de datos personales.
* Evaluaciones del impacto de los cambios tecnológicos implementados en la Entidad.
* Lecciones aprendidas de incidentes relacionados con la seguridad y privacidad de los datos personales.

Toda revisión debe ser documentada, aprobada por las instancias correspondientes, y comunicada a las partes interesadas mediante los canales oficiales.

## Política de continuidad del negocio o del sistema de gestión y continuidad del negocio (SGCN)

**Objetivo de la Política**

El objetivo de esta política es establecer los lineamientos necesarios para garantizar la resiliencia operativa del Ministerio de Minas y Energía (MINENERGÍA) frente a incidentes, emergencias o desastres que puedan interrumpir sus funciones críticas. La política busca asegurar que las operaciones esenciales del Ministerio continúen en niveles aceptables, minimizando el impacto en los servicios, protegiendo los activos críticos y cumpliendo con las obligaciones legales, contractuales y misionales.

En particular, esta política se enfoca en:

1. Brindar orientación y apoyo desde la Alta Dirección para fortalecer la capacidad de respuesta ante incidentes.
2. Proteger la integridad, confidencialidad y disponibilidad de la información durante situaciones adversas.
3. Asegurar que los procesos críticos puedan reanudarse dentro de los tiempos definidos en el análisis de impacto al negocio (BIA).

Esta política estará disponible en forma documentada para todas las partes interesadas internas y externas, y será accesible a través de diferentes canales de comunicación institucional.

**Compromiso del Ministerio de Minas y Energía**

Se compromete a:

1. Identificar los requisitos de continuidad de la información y los procesos misionales esenciales, considerando las amenazas internas y externas.
2. Diseñar, implementar y mantener un Sistema de Gestión de Continuidad del Negocio (SGCN) basado en estándares internacionales como ISO 22301.
3. Establecer procedimientos de respuesta para minimizar el tiempo de interrupción de los servicios críticos y facilitar el retorno a la normalidad tras un incidente.
4. Realizar ejercicios regulares de simulación y pruebas del SGCN para garantizar su eficacia.
5. Asignar los recursos necesarios (humanos, tecnológicos y financieros) para asegurar la implementación y mejora continua del SGCN.

**Principios Fundamentales de Continuidad del Negocio**

El SGCN del Ministerio de Minas y Energía se basa en los siguientes principios:

1. **Resiliencia Operativa:** Fortalecer los procesos críticos para soportar interrupciones imprevistas.
2. **Proporcionalidad:** Asegurar que los controles y procedimientos de continuidad sean proporcionales al nivel de riesgo asociado.
3. **Integración:** Incorporar la continuidad del negocio como parte del ciclo de vida de los procesos y tecnologías de la Entidad.
4. **Eficiencia:** Optimizar recursos para la implementación de planes y estrategias de continuidad.
5. **Mejora Continua:** Revisar y actualizar regularmente los planes de continuidad para reflejar cambios en el entorno interno y externo.

**Alcance/Aplicabilidad**

Esta política aplica a:

1. Todos los funcionarios, colaboradores, contratistas y proveedores que realicen actividades relacionadas con los procesos del Ministerio.
2. Los sistemas de información, infraestructura tecnológica, procesos críticos y activos relacionados identificados en el BIA.
3. Las instalaciones físicas y virtuales utilizadas para soportar las operaciones críticas del Ministerio.
4. Todos los niveles jerárquicos, garantizando que la continuidad del negocio sea una responsabilidad compartida y transversal.

Esta política es aplicable a los incidentes causados por fallos tecnológicos, desastres naturales, ataques cibernéticos, pandemias, fallos de suministro, entre otros riesgos identificados en la matriz de análisis de riesgos.

**Responsabilidades**

1. **Alta Dirección:** Garantizar el liderazgo, apoyo y asignación de recursos necesarios para implementar y mantener el SGCN.
2. **Oficial de Continuidad del Negocio:** Supervisar la gestión del SGCN, coordinar simulacros, pruebas y auditorías, y garantizar el cumplimiento de esta política.
3. **Oficial de Seguridad de la Información:** Coordinar la integración de la continuidad de la información en los planes generales de continuidad del negocio.
4. **Mesas de Trabajo:** Asegurar la revisión y aprobación de cambios significativos en el SGCN y evaluar los planes de acción derivados de pruebas y simulacros.
5. **Líderes de Procesos Críticos:** Identificar y mantener actualizados los requisitos de continuidad de los procesos críticos.

**Nivel de Cumplimiento de la Política**

El cumplimiento de esta política es obligatorio para todas las personas, procesos y áreas identificadas dentro de su alcance. El incumplimiento será tratado como una falta grave y puede resultar en medidas disciplinarias o legales, según lo establecido en los reglamentos internos y normativas aplicables.

El monitoreo del cumplimiento se realizará a través de auditorías internas, ejercicios de simulación y revisiones periódicas.

**Excepciones a la Política**

Cualquier excepción o modificación a esta política debe ser:

1. Solicitada de forma documentada.
2. Aprobada por el Oficial de Continuidad del Negocio y el Oficial de Seguridad de la Información o quien haga sus veces.
3. Revisada por la mesa de trabajo de gestión de cambios y continuidad del negocio.

Las excepciones aprobadas deben ser revisadas periódicamente para garantizar que no representen riesgos significativos para la Entidad.

**Revisiones**

Esta política será revisada al menos una vez al año o cuando ocurran las siguientes circunstancias:

1. Cambios en las normativas o estándares aplicables.
2. Incidentes significativos que afecten la continuidad del negocio o de la información.
3. Cambios en los procesos, sistemas o infraestructura crítica del Ministerio.
4. Lecciones aprendidas de simulacros o eventos reales de interrupción.

Las revisiones serán aprobadas por la Alta Dirección y comunicadas oportunamente a las partes interesadas.

### Política de Recuperación ante Desastres TIC

**Objetivo de la Política**

El Ministerio de Minas y Energía dedicará los esfuerzos necesarios y suficientes para reducir la probabilidad de interrupciones en sus operaciones relacionadas con las Tecnologías de la Información y las Comunicaciones (TIC). En caso de interrupciones, esta política asegura que estas no excedan los objetivos de tiempo de recuperación (RTO) y que se garanticen los recursos necesarios para la restauración oportuna de los servicios críticos.

La política tiene como propósito implementar un marco de gestión de la continuidad de la operación de TIC con énfasis en actividades críticas identificadas durante el Análisis de Impacto al Negocio (BIA). Además, se busca mantener la integridad, disponibilidad y confidencialidad de los sistemas de información, incluso durante situaciones adversas.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, incluyendo:

* Los usuarios, colaboradores, contratistas y proveedores que interactúan con los sistemas y servicios TIC del Ministerio de Minas y Energía.
* Los sistemas de información, infraestructura tecnológica, aplicaciones críticas y servicios de soporte TIC identificados como esenciales.
* Las instalaciones físicas y virtuales que soportan las operaciones TIC del Ministerio.
* Los procesos de gestión y recuperación que integran el Sistema de Gestión de la Continuidad del Negocio (SGCN) y el Sistema de Gestión de Seguridad de la Información (SGSI).

**Principios de la Recuperación ante Desastres TIC**

1. **Preparación Proactiva:** Reducir la probabilidad de fallos e interrupciones mediante la implementación de controles preventivos y planes de contingencia.
2. **Resiliencia Operativa:** Garantizar que los sistemas críticos puedan ser restaurados en los tiempos definidos (RTO y RPO).
3. **Colaboración Efectiva:** Coordinar las actividades de recuperación entre todas las áreas involucradas, incluidos el Grupo TIC, contratistas y dependencias operativas.
4. **Pruebas y Validaciones:** Realizar simulacros periódicos para validar la efectividad y pertinencia de los planes de recuperación.
5. **Mejora Continua:** Incorporar lecciones aprendidas y actualizaciones tecnológicas para fortalecer la recuperación ante desastres TIC.

**Responsabilidades para la Gestión de la Recuperación Ante Desastres TIC**

1. **Administrador del Centro de Cómputo**
2. Garantiza que los Planes de Recuperación ante Desastres TIC se implementen de acuerdo con esta política.
3. Asegura la disponibilidad de recursos necesarios para las actividades de recuperación.
4. **Grupo TIC**
5. Revisa los Planes de Recuperación ante Desastres TIC al menos una vez al año o cuando ocurran cambios significativos.
6. Realiza simulacros de recuperación dos veces al año, documentando los resultados y recomendaciones.
7. Mantiene actualizados los procedimientos operativos relacionados con la continuidad de TIC.
8. **Secretaría General:**
9. Promueve el desarrollo e implementación de programas para la gestión de recursos humanos, financieros y tecnológicos.
10. Coordina la implementación de la Gestión de Continuidad de la Operación de TIC bajo la presente política.
11. **Mesa de trabajo de gestión de cambios y continuidad del negocio**
12. Revisa el Sistema de Gestión de la Continuidad de la Operación de TIC (SGCN) al menos una vez al año o tras cambios significativos.
13. Emite informes para garantizar la eficacia y adecuación del SGCN.
14. **Outsourcing de Administración Tecnológica:**
15. En casos aplicables, participa en la implementación y mantenimiento del SGCN bajo la supervisión del Administrador del Centro de Cómputo.

**Nivel de Cumplimiento de la Política**

Todas las personas y entidades cubiertas por el alcance de esta política deben garantizar el 100% de cumplimiento de los lineamientos establecidos.

El monitoreo del cumplimiento se realizará mediante auditorías internas, simulacros y evaluaciones periódicas. Los incumplimientos serán tratados como faltas graves y estarán sujetos a medidas correctivas, disciplinarias o legales según corresponda.

**Excepciones a la Política**

Cualquier excepción a esta política deberá:

Ser justificada y documentada por el área solicitante y contar con la aprobación del Oficial de Seguridad de la Información y/o quien haga sus veces, además de ser revisada por la mesa de trabajo de gestión de cambios y continuidad del negocio.

**Revisiones**

Esta política será revisada en las siguientes situaciones:

1. Anualmente, para evaluar su pertinencia y eficacia.
2. Cuando ocurran cambios significativos en la infraestructura TIC o en los procesos críticos del Ministerio.
3. Tras la aparición de nuevas normativas o estándares aplicables a la recuperación ante desastres TIC.
4. Después de simulacros, auditorías o incidentes relevantes, incorporando las lecciones aprendidas.
5. Las revisiones serán lideradas por el Grupo TIC, con el apoyo del Administrador del Centro de Cómputo, y aprobadas por la Mesa de Trabajo de Gestión de Cambios y Continuidad del Negocio.

**Detalle de la Implementación**

La implementación de esta política se detalla en el documento **plan para la Recuperación de Desastres de los Servicios que presta el Grupo TIC del Ministerio de Minas y Energía (DRP)**, que incluye:

1. Procedimientos específicos para restaurar servicios TIC en tiempos aceptables.
2. Estrategias de respaldo de información y sitios alternos para garantizar la continuidad operativa.
3. Roles y responsabilidades específicas para cada etapa del proceso de recuperación.
4. Protocolos de comunicación para coordinar las actividades de recuperación y mantener informadas a las partes interesadas.

## Políticas de seguridad y privacidad de la información

El Ministerio de Minas y Energía adopta políticas de seguridad y privacidad de la información para garantizar la protección integral de sus activos de información frente a riesgos internos y externos. Estas políticas establecen directrices claras para salvaguardar la confidencialidad, integridad y disponibilidad de la información, alineándose con los estándares internacionales como ISO/IEC 27001 y las normativas locales aplicables.

Las políticas incluyen la clasificación de la información, la gestión de accesos, el uso adecuado de recursos tecnológicos, la protección contra incidentes de seguridad y la privacidad de los datos personales, asegurando que todos los usuarios internos y externos actúen conforme a los principios de ética y responsabilidad. Además, estas directrices fomentan una cultura organizacional basada en la seguridad, estableciendo controles específicos y procedimientos documentados para prevenir, detectar y responder a posibles amenazas.

### 7.2.1 Política para gestión de riesgos de Seguridad de la Información

El Ministerio de Minas y Energía adopta la guía para la administración del riesgo elaborada por el Departamento Administrativo de la Función Pública (DAFP), basada en la norma internacional ISO 31000 para la gestión de riesgos. Este enfoque se complementa con el Procedimiento de Administración del Riesgo de la Entidad, asegurando un marco integral que facilite la identificación, evaluación, tratamiento y monitoreo de los riesgos asociados con la seguridad de la información.

Los riesgos de seguridad de la información identificados deben ser gestionados de manera adecuada para minimizar su impacto y probabilidad de ocurrencia. Cada riesgo será objeto de seguimiento trimestral por parte del líder o dueño del proceso correspondiente, garantizando que las medidas de tratamiento implementadas sean efectivas y cumplan con los objetivos establecidos. Además, estos riesgos serán incorporados en todas las matrices de riesgos de los procesos de la Entidad, asegurando su alineación con las estrategias de gestión organizacional.

La mesa de trabajo de seguridad y privacidad de la información se encargará de analizar y tratar los riesgos identificados, documentando el seguimiento a través de registros formales al menos dos veces al año. Este proceso permitirá evaluar la conveniencia y efectividad de las acciones implementadas para mitigar los riesgos y fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI).

En caso de adquirir nuevas tecnologías o soluciones de seguridad informática, estas deberán estar justificadas con base en los resultados de los análisis de riesgos previamente realizados. Esto garantizará que las inversiones respondan a necesidades reales y proporcionen beneficios claros en términos de mitigación o tratamiento de los riesgos identificados.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, sus usuarios, colaboradores, contratistas y proveedores, así como a cualquier ciudadano que utilice o interactúe con activos de información propiedad del Ministerio de Minas y Energía.

**Nivel de Cumplimiento de la Política**

El cumplimiento del 100% de esta política es obligatorio para todas las personas y áreas cubiertas por su alcance y aplicabilidad.

Excepciones a la Política

Cualquier modificación a esta política deberá ser escalada al Oficial de Seguridad de la Información y/o a quien haga sus veces. La mesa de trabajo de seguridad y privacidad de la información será responsable de revisar y validar dichas modificaciones.

**Revisiones**

La política será revisada anualmente o cuando ocurran cambios significativos en los componentes del SGSI, del SGCN, del MSPI, o en las condiciones internas y externas que puedan afectar la gestión de riesgos del Ministerio. Estas revisiones garantizarán que la política se mantenga relevante y alineada con las necesidades y objetivos organizacionales.

### 7.2.2 Política de separación de deberes

**Objetivo de la Política**

Establecer la separación de deberes y áreas de responsabilidad dentro del Ministerio de Minas y Energía para reducir las posibilidades de modificación no autorizada, errores no intencionales o uso indebido de los activos de información. Esta política asegura que las tareas críticas sean distribuidas entre múltiples roles, fortaleciendo el control interno y la transparencia en el manejo de los activos.

**Directrices de la Política**

La implementación de esta política se fundamenta en los siguientes principios clave:

* 1. **Necesidad de saber**

El acceso a la información estará restringido únicamente a aquellas personas que lo requieran por razones justificadas de negocio y cuenten con autorización explícita. Se configurarán permisos de acceso que, en lo posible, permitan solo lectura. Los usuarios con permisos para efectuar cambios sobre la información serán limitados al mínimo necesario.

* 1. **Menor Privilegio**

Todos los usuarios tendrán el menor nivel de acceso requerido para desempeñar sus funciones. Por defecto, el acceso estará denegado, y se habilitará únicamente lo estrictamente necesario. La premisa operativa es: "En general, todo está prohibido, a menos que se permita expresamente".

* 1. **Separación de deberes**

Para minimizar los riesgos de abuso o errores, las tareas sobre los activos de información estarán distribuidas. Por ejemplo, una persona será responsable de iniciar los procesos, otra de probarlos o autorizarlos, y una tercera de auditar o finalizar las operaciones. Este enfoque obliga a la colaboración de múltiples roles, áreas y procesos.

* 1. **Rotación de trabajo**

Los deberes y roles de los colaboradores se rotarán periódicamente, varias veces al año, para mejorar la seguridad, garantizar la integridad operativa, fortalecer la moral del equipo y asegurar la continuidad de los procesos críticos.

* 1. **Cuidado necesario y debida diligencia**

El Ministerio actuará en cumplimiento de la legislación aplicable y las demandas de las partes interesadas. Esto incluye esfuerzos demostrables para aplicar las mejores prácticas y garantizar que las tareas se lleven a cabo bajo estrictos estándares de cuidado y seguridad.

* 1. **Gestión de usuarios con altos privilegios**

Los usuarios con privilegios elevados, como aquellos que autorizan accesos, transacciones o procesos críticos, serán objeto de auditorías y supervisión. Este monitoreo estará a cargo de un designado de las Mesas de Trabajo y/o de quien haga sus veces, con el objetivo de asegurar el uso adecuado de sus privilegios.

En el diseño de los controles se considerará la posibilidad de confabulación, especialmente en situaciones donde la separación total de deberes sea difícil de implementar. En tales casos, se adoptarán medidas adicionales, como el seguimiento de actividades, la generación de rastros de auditoría y la supervisión directa por parte de la dirección.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, incluyendo los usuarios, colaboradores, contratistas y terceros que interactúen con los activos de información del Ministerio de Minas y Energía. Asimismo, incluye a cualquier persona o entidad que utilice dichos activos.

**Nivel de Cumplimiento de la Política**

El cumplimiento de esta política es obligatorio para todas las personas incluidas en su alcance. Se exige un cumplimiento del 100%, y se realizarán auditorías periódicas para verificar la adherencia a las directrices.

**Excepciones a la Política**

Cualquier solicitud de excepción a esta política debe ser documentada y escalada al Oficial de Seguridad de la Información y/o quien haga sus veces. Las excepciones serán revisadas y validadas por la Mesa de Seguridad y Privacidad de la Información.

R**evisiones**

Esta política será revisada anualmente o cuando ocurra un cambio significativo en el Sistema de Gestión de Seguridad de la Información (SGSI), el Sistema de Gestión de Continuidad del Negocio (SGCN), el Modelo de Seguridad y Privacidad de la Información (MSPI), o en las condiciones internas y externas del Ministerio que puedan impactar la gestión de riesgos.

### 7.2.3 Política de contacto con autoridades de seguridad de la información

**Objetivo de la Política**

Mantener contactos apropiados con las autoridades y organismos pertinentes para gestionar de manera eficiente los temas relacionados con la Seguridad de la Información y el Sistema de Gestión de Seguridad de la Información (SGSI). Esto incluye la colaboración activa en la prevención, manejo y resolución de incidentes de seguridad, garantizando el cumplimiento de las leyes y normativas aplicables.

**Marco Legal y Relevancia**

En Colombia, la Ley 1273 de 2009, conocida como Ley de Delitos Informáticos, protege como bien jurídico la información y los datos. Esta norma tipifica diversos delitos relacionados con la protección de la información, incluyendo conductas que afectan el patrimonio económico, como el hurto por medios informáticos y la transferencia no consentida de activos. El cibercrimen, definido como las actividades ilegales relacionadas con el uso de tecnologías de información y comunicación, representa una amenaza directa contra la confidencialidad, integridad y disponibilidad de la información, así como contra los sistemas informáticos y la infraestructura de las organizaciones.

**Lineamientos Generales**

El Ministerio de Minas y Energía mantendrá y actualizará, según sea necesario, los canales de comunicación establecidos con autoridades y organismos especializados para gestionar incidentes, reportar eventos e intercambiar información relacionada con la seguridad de la información, la ciberseguridad y la seguridad digital. Dichos contactos estarán alineados con los procesos misionales del Ministerio y las necesidades específicas derivadas de la información que procesa, almacena y transmite.

Se destacan los siguientes organismos y contactos:

1. **COLCERT:** Grupo de Respuesta a Emergencias Cibernéticas en Colombia, encargado de la coordinación de la ciberseguridad y ciberdefensa nacional, protegiendo la infraestructura crítica del Estado.
2. **CSIRT-PONAL:** Equipo de la Policía Nacional para la prevención, atención e investigación de incidentes de seguridad informática.
3. **CSIRT-Presidencia:** Equipo de la Presidencia para la prevención, atención e investigación de incidentes de seguridad informática.
4. **C4 (Comando conjunto cibernético policial):** Dependencia de la Dirección de Investigación Criminal , especializada en estrategias contra delitos que afectan la información y los datos.
5. **Liga Colombiana de Radioaficionados (L.C.R.A.):** Colabora en casos de calamidades públicas y emergencias relacionadas con las TIC, en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones.
6. **Infraestructura de Firma Digital:** Entidades como Certicámara, GSE y Andes SCD brindan servicios de emisión de certificados digitales y asesoramiento en tecnologías relacionadas con firma digital y documentos electrónicos.
7. **Superintendencia de Industria y Comercio:** Entidad encargada de la protección al consumidor, propiedad industrial y competencia, con relevancia para la protección de datos.
8. **Dirección Nacional de Derecho de Autor:** Responsable del registro y la protección de obras literarias, artísticas y contratos relacionados, proporcionando seguridad jurídica en el ámbito de derechos de autor.

**Confidencialidad y Manejo de Información**

En los intercambios de información sobre Seguridad de la Información, no se divulgará información confidencial del Ministerio de Minas y Energía a personas no autorizadas. Cualquier intercambio de información confidencial requerirá la firma de un Compromiso de Confidencialidad previo, o deberá realizarse exclusivamente con organizaciones especializadas cuyo personal esté obligado a mantener la confidencialidad.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, incluidos los usuarios, colaboradores, contratistas y cualquier persona que utilice o tenga relación con los activos de información del Ministerio de Minas y Energía.

**Nivel de Cumplimiento de la Política**

El cumplimiento del 100% de esta política es obligatorio para todas las personas cubiertas por su alcance. Auditorías y controles periódicos verificarán el cumplimiento efectivo.

**Excepciones a la Política**

Cualquier modificación o excepción a esta política deberá ser escalada al Oficial de Seguridad de la Información y revisada por la Mesa de Seguridad y Privacidad de la Información.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en el SGSI, el SGCN, el MSPI, en las partes interesadas o en los procesos internos de la Entidad. Estas revisiones garantizarán su relevancia y eficacia frente a los cambios normativos o tecnológicos.

### 7.2.3 Política de gestión de grupos de interés especial

**Objetivo de la Política**

Establecer y mantener contactos adecuados con grupos de interés especial, foros y asociaciones profesionales especializadas en Seguridad de la Información y Ciberseguridad. Estos vínculos permiten al Ministerio de Minas y Energía mantenerse actualizado con las mejores prácticas, identificar nuevas amenazas, acceder a asesorías especializadas y fortalecer su entorno de seguridad.

**Directrices de la Política**

El Ministerio de Minas y Energía, a través del responsable de Seguridad de la Información, gestionará la suscripción y participación en comunidades, entidades y organismos relevantes en materia de Seguridad de la Información. Esto se realiza con los siguientes propósitos:

* **Mejorar el conocimiento técnico y estratégico:** Participar en estas redes permitirá identificar mejores prácticas, mantenerse al día con la evolución de la tecnología y comprender nuevas amenazas y vulnerabilidades.
* **Obtener alertas y advertencias tempranas:** Recibir información actualizada sobre parches, avisos de vulnerabilidades y posibles ataques para tomar decisiones oportunas y proactivas.
* **Acceder a asesoramiento especializado:** Disponer de fuentes confiables de consulta técnica y estratégica para enfrentar desafíos en Seguridad de la Información.
* **Fomentar el intercambio de información:** Compartir experiencias, conocimientos y estrategias relacionadas con nuevas tecnologías, productos y soluciones para proteger los activos del Ministerio.
* **Establecer puntos de contacto para incidentes:** Contar con enlaces apropiados para gestionar incidentes de seguridad con rapidez y eficacia.

El Ministerio se suscribirá y consultará regularmente fuentes confiables y organizaciones reconocidas, tales como:

* **NIST:** Referencia clave para normas, guías y buenas prácticas en ciberseguridad.
* **Fabricantes de tecnología:** Boletines de seguridad de proveedores de infraestructura tecnológica y software.
* **INCIBE:** Instituto Nacional de Ciberseguridad de España, una fuente confiable de alertas y asesorías técnicas.
* **CVE y bases de datos asociadas:** Plataformas como <https://cve.mitre.org> y <https://www.cve.org> para el monitoreo de vulnerabilidades identificadas.
* **Otros foros y asociaciones especializadas:** Dependiendo de la evolución tecnológica y necesidades específicas de la Entidad.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, incluidos los usuarios, colaboradores, contratistas y cualquier persona o grupo que tenga relación con los activos de información del Ministerio de Minas y Energía. También se extiende a los equipos responsables de tomar decisiones estratégicas y técnicas en materia de seguridad.

**Nivel de Cumplimiento de la Política**

El cumplimiento de esta política es obligatorio y debe ser garantizado por todas las personas y áreas bajo su alcance. Se realizará un monitoreo periódico para verificar la participación activa y el aprovechamiento de las redes de interés especial.

**Excepciones a la Política**

Cualquier excepción o modificación a esta política deberá ser documentada y aprobada por el Oficial de Seguridad de la Información o quien haga sus veces. Además, estas modificaciones serán revisadas y validadas por la mesa de seguridad y privacidad de la Información o quien haga sus pares.

**Revisiones**

Esta política será revisada de forma anual o cuando ocurran cambios significativos en los componentes del SGSI, SGCN, MSPI o en las condiciones internas y externas que afecten los objetivos del Ministerio. Las revisiones garantizarán que la política siga siendo relevante, efectiva y alineada con las mejores prácticas y necesidades organizacionales.

### 7.2.4 Política de Seguridad de la Información en la Gestión de Proyectos

**Objetivo de la política**

Integrar la Seguridad de la Información en todas las etapas de la gestión de proyectos, asegurando que los riesgos asociados sean identificados, evaluados y tratados desde la planeación inicial hasta la finalización del proyecto. Este enfoque tiene como propósito proteger los activos de información del Ministerio de Minas y Energía y garantizar que los proyectos cumplan con los estándares de seguridad requeridos.

**Directrices de la política**

En la gestión de proyectos dentro del Ministerio de Minas y Energía, se deben cumplir los siguientes lineamientos:

1. **Incorporación de la Seguridad de la Información en los Objetivos del Proyecto:**  
   Los objetivos relacionados con la Seguridad de la Información deben estar claramente definidos e integrados en los objetivos generales de cada proyecto, asegurando que se consideren aspectos como la confidencialidad, integridad y disponibilidad de los datos y activos involucrados.
2. **Valoración Temprana de Riesgos:** La identificación y evaluación de los riesgos de seguridad de la información se realizarán en una etapa temprana del proyecto, permitiendo la implementación de controles adecuados para mitigar dichos riesgos y garantizar el éxito del proyecto. Esta valoración debe ser actualizada a medida que el proyecto avanza y su entorno cambia.
3. **Seguridad en Todas las Fases del Proyecto:** La Seguridad de la Información debe ser integrada en todas las fases de la metodología de gestión de proyectos, desde la planeación y diseño, pasando por la ejecución y pruebas, hasta la entrega y cierre. Cada fase debe incluir actividades específicas relacionadas con la identificación de riesgos, la implementación de controles y la validación de medidas de seguridad.
4. **Capacitación y Concienciación del Personal del Proyecto:** Los equipos de proyecto recibirán orientación y capacitación sobre los requisitos de seguridad aplicables, asegurando que comprendan su rol en la protección de los activos de información y en el cumplimiento de los estándares establecidos.
5. **Documentación y Monitoreo:** La documentación de los aspectos de seguridad en la gestión del proyecto es obligatoria, incluyendo los análisis de riesgos, las acciones correctivas y las auditorías de cumplimiento. Además, se deben monitorear de manera continua los controles implementados para garantizar su eficacia.

**Alcance/Aplicabilidad**

Esta política aplica a todos los proyectos desarrollados o gestionados por la Entidad, incluyendo a los usuarios, colaboradores, contratistas y proveedores que tengan relación o utilicen activos de información del Ministerio de Minas y Energía. Asimismo, es aplicable a cualquier proceso que involucre la adquisición, desarrollo o implementación de soluciones tecnológicas.

**Nivel de cumplimiento de la política**

El cumplimiento del 100% de esta política es obligatorio para todas las personas y áreas cubiertas por su alcance. Auditorías internas y revisiones periódicas garantizarán la adherencia a los lineamientos establecidos.

**Excepciones a la política**

Cualquier solicitud de modificación o excepción a esta política deberá ser documentada y escalada al Oficial de Seguridad de la Información o a quien haga sus veces. La Mesa de Seguridad y Privacidad de la Información será responsable de revisar y validar dichas excepciones.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los componentes del SGSI, SGCN, MSPI, o en las condiciones internas o externas que impacten los proyectos gestionados por la Entidad. Estas revisiones tienen como objetivo mantener la vigencia, eficacia y alineación de la política con las mejores prácticas de la industria.

### 7.2.5 Política de dispositivos móviles

**Objetivo de la política**

Promover el uso adecuado y seguro de los dispositivos móviles y las actividades de teletrabajo, garantizando niveles adecuados de confidencialidad, integridad y disponibilidad para proteger la información crítica o sensible almacenada, transmitida o transportada a través de dispositivos móviles, removibles o canales de comunicación.

**Directrices de la Política**

El Ministerio de Minas y Energía adopta las siguientes directrices para la gestión de dispositivos móviles institucionales y personales utilizados en sus operaciones:

1. **Gestión y Control de Dispositivos Móviles:**

El Ministerio controlará y gestionará los dispositivos móviles institucionales (como teléfonos inteligentes, portátiles, discos duros, USB y DVD) que accedan a sistemas de información o equipos de la Entidad. Su manejo será aprobado previamente por el Oficial de Seguridad de la Información y/o quien haga sus veces.

1. **Configuración y protección de dispositivos:**
   * El Oficial de Seguridad de la Información definirá los requisitos mínimos de protección, configuraciones aceptables y herramientas de seguridad (como antimalware) para los dispositivos móviles institucionales.
   * Los dispositivos móviles deberán estar cifrados, asegurando que los datos almacenados no puedan ser copiados o extraídos sin el método de desbloqueo correspondiente.
   * Se configurará la opción de borrado remoto para eliminar los datos en caso de pérdida o robo, evitando divulgaciones no autorizadas.
2. **Respaldo y Almacenamiento de Información:**
   * El Grupo TIC garantizará la realización de copias de seguridad de la información almacenada en los dispositivos móviles institucionales.
   * Los usuarios no deben almacenar información personal, videos o fotografías en dispositivos asignados por la Entidad.
3. **Uso Seguro de Dispositivos:**
   * Los dispositivos no deben conectarse a puertos USB en lugares no autorizados como hoteles, aeropuertos, o cibercafés.
   * Se prohíbe la modificación de configuraciones de seguridad, la desinstalación de software autorizado o la instalación de programas no autorizados.
   * Cualquier intento de uso no autorizado será considerado una violación grave de esta política y será sujeto a sanciones según lo establecido en las normativas internas.
4. **Gestión de Dispositivos Personales:**
   * Los dispositivos personales utilizados para acceder a sistemas o información del Ministerio deberán estar gestionados mediante una solución de Administración de Dispositivos Móviles (MDM) implementada por la Entidad.
5. **Registro y Supervisión:**
   * Todos los dispositivos institucionales serán registrados y formalmente asignados, asegurando que los usuarios acepten los requisitos de protección física y las responsabilidades asociadas.
   * El uso de dispositivos será monitoreado regularmente para garantizar el cumplimiento de las políticas y la seguridad de la información.

**Alcance/Aplicabilidad**

Esta política aplica a todos los dispositivos móviles utilizados por la Entidad, sus usuarios, colaboradores, contratistas y cualquier persona que maneje información o activos propiedad del Ministerio de Minas y Energía.

**Nivel de Cumplimiento de la Política**

El cumplimiento del 100% de esta política es obligatorio para todas las personas incluidas en su alcance. Auditorías internas y controles periódicos garantizarán la adherencia a estas directrices.

**Excepciones a la política**

Cualquier modificación o excepción deberá ser documentada y aprobada por el Oficial de Seguridad de la Información y/o quien haga sus veces. Las excepciones serán revisadas por la Mesa de Seguridad y Privacidad de la Información.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en el SGSI, SGCN, MSPI, en las partes interesadas, o en los procesos internos de la Entidad. Estas revisiones asegurarán que la política siga siendo efectiva y relevante frente a los cambios tecnológicos y normativos.

### 7.2.6 Política BYOD (Bring Your Own Device)

**Objetivo de la política**

Regular el uso de dispositivos personales de las partes interesadas dentro de las instalaciones del Ministerio de Minas y Energía, garantizando que dicho uso no comprometa la seguridad de la información ni los activos tecnológicos de la Entidad. Esta política busca establecer lineamientos claros para el manejo, acceso y control de dispositivos personales en el entorno institucional.

**Directrices de la política**

El acceso físico y lógico a las instalaciones y a la red del Ministerio de Minas y Energía por parte de dispositivos personales (como portátiles, tabletas, notebooks y otros) estará estrictamente controlado. Dicho acceso será registrado, aprobado previamente y validado por el Oficial de Seguridad de la Información o quien haga sus veces, en conjunto con el Grupo TIC.

El Ministerio implementará campañas de concienciación para las partes interesadas sobre las buenas prácticas de seguridad informática, tales como el aseguramiento físico de los dispositivos, la protección de equipos desatendidos y el cumplimiento de los requerimientos mínimos de Seguridad de la Información, que incluyen el uso de software antivirus y la aplicación regular de actualizaciones de parches.

**Responsabilidades relacionadas con los dispositivos**

* **Exclusión de responsabilidad:** El Ministerio de Minas y Energía no asume responsabilidad alguna por daños, pérdida o robo de los dispositivos personales que ingresen a sus instalaciones. Asimismo, no se hará responsable por la información contenida en dichos dispositivos.
* **Revisión de dispositivos**: En caso necesario, los dispositivos personales podrán ser sujetos a revisión o investigación previa autorización por escrito de su propietario.
* **Soporte técnico:** El Grupo TIC no proporcionará apoyo técnico ni soporte a dispositivos personales bajo ninguna circunstancia.

**Uso responsable de tecnología**

* **Contraseñas seguras:** Los usuarios deberán utilizar contraseñas complejas, seguras y no compartirlas bajo ningún motivo.
* **Conexión a la red institucional:** Los dispositivos personales que requieran conectarse a la red inalámbrica del Ministerio deberán justificar su uso, y la solicitud deberá ser validada y aprobada por el Oficial de Seguridad de la Información o quien haga sus veces.
* **Licencias de software:** Todo software instalado en los dispositivos personales utilizados para acceder a sistemas o activos de información de la Entidad deberá contar con las licencias adecuadas y estar en cumplimiento con las normativas de propiedad intelectual.
* **Cumplimiento de políticas:** Las partes interesadas deberán cumplir con todas las políticas de Seguridad de la Información del Ministerio de Minas y Energía, garantizando que sus acciones no comprometan la seguridad de los activos tecnológicos y la información de la Entidad.

**Alcance/Aplicabilidad**

Esta política aplica a todas las personas, incluidas las partes interesadas, usuarios y colaboradores del Ministerio de Minas y Energía, que tengan relación con los activos de información de la Entidad o utilicen dispositivos personales en sus instalaciones o redes.

**Nivel de cumplimiento de la política**

El cumplimiento del 100% de esta política es obligatorio para todas las personas y áreas incluidas en su alcance. La supervisión del cumplimiento se realizará mediante auditorías y controles periódicos.

**Excepciones a la política**

Cualquier solicitud de modificación o excepción a esta política deberá ser documentada, escalada al Oficial de Seguridad de la Información y revisada por la Mesa de Seguridad y Privacidad de la Información.

**Revisiones**

Esta política será revisada de manera anual o cuando ocurran cambios significativos en el SGSI, SGCN, MSPI, o en las condiciones internas o externas de la Entidad que puedan impactar su cumplimiento o pertinencia.

**7.2.7 Política para teletrabajo y trabajo remoto**

**Objetivo de la política**

Establecer medidas de seguridad para proteger la información que es accedida, procesada o almacenada durante las actividades de teletrabajo o trabajo remoto. La política define condiciones, controles y restricciones necesarias para garantizar la seguridad de los activos de información del Ministerio de Minas y Energía en estos entornos, alineándose con la Ley 1221 de 2008 y las políticas del SGSI.

**Directrices de la política**

El Ministerio de Minas y Energía establece las siguientes directrices para las actividades de teletrabajo y trabajo remoto:

1. **Protección física y lógica del entorno de teletrabajo:** El lugar en el que se desarrollen las actividades de teletrabajo deberá contar con condiciones adecuadas de seguridad física, previniendo el hurto, daño o pérdida de equipos e información. Asimismo, las conexiones utilizadas deberán estar protegidas contra accesos no autorizados y divulgaciones indebidas de información.
2. **Autorización previa de teletrabajo:** El Oficial de Seguridad de la Información o quien haga sus veces, autorizará las actividades de teletrabajo una vez que se implementen los controles de seguridad requeridos, asegurando que se cumplan las normativas aplicables y las políticas del SGSI.
3. **Requisitos de seguridad para los equipos:** Los dispositivos utilizados para el teletrabajo deberán contar con protección de antivirus actualizados, firewall configurado, y otras soluciones de seguridad aprobadas por el Grupo TIC para salvaguardar la información de la Entidad.
4. **Definición de alcance y condiciones de teletrabajo:** Antes de iniciar el teletrabajo, se definirán formalmente los objetivos del trabajo, la información y sistemas que serán accedidos, y el horario permitido. Todo ello será documentado y aprobado por el Oficial de Seguridad de la Información o quien haga sus veces.
5. **Monitoreo y auditoría de conexiones remotas:** El Oficial de Seguridad de la Información realizará revisiones periódicas de las conexiones remotas, verificando el cumplimiento de las medidas de seguridad establecidas. Emitirá recomendaciones para mitigar riesgos identificados durante estas revisiones.
6. **Capacitación y concienciación:** Se implementarán programas de sensibilización dirigidos a las partes interesadas para fomentar el uso adecuado de las herramientas tecnológicas, la protección de la información y el cumplimiento de las políticas de seguridad en teletrabajo.

**Alcance/aplicabilidad**

Esta política aplica a todos los usuarios, colaboradores, contratistas y demás partes interesadas que desarrollen actividades de teletrabajo o trabajo remoto, utilizando activos de información o sistemas del Ministerio de Minas y Energía.

**Nivel de cumplimiento de la política**

El cumplimiento del 100% de esta política es obligatorio para todas las personas y áreas bajo su alcance. Auditorías y controles periódicos garantizarán la adherencia a los lineamientos establecidos.

**Excepciones a la política**

Cualquier solicitud de modificación o excepción deberá ser documentada, aprobada por el Oficial de Seguridad de la Información y revisada por la Mesa de Seguridad y Privacidad de la Información.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los componentes del SGSI, SGCN, MSPI, o en las condiciones internas y externas de la Entidad que impacten las actividades de teletrabajo.

### 7.2.8 Política de gestión humana

**Objetivo de la política**

Garantizar que los empleados y contratistas del Ministerio de Minas y Energía comprendan sus responsabilidades, sean idóneos para los roles asignados y cumplan con los requisitos de seguridad establecidos para proteger los activos de información a lo largo de todo el ciclo laboral: selección, vinculación, desempeño y finalización de su relación laboral o contractual.

**Directrices de la política**

El Ministerio de Minas y Energía implementará controles en todas las etapas del ciclo de vida laboral, como se detalla a continuación:

* 1. **Procesos de selección**
* **Verificación de antecedentes:** La Subdirección de Talento Humano verificará que los documentos y referencias presentados por los candidatos sean verídicos y estén alineados con los requisitos del cargo. Esto incluye antecedentes laborales, penales y financieros, según la sensibilidad del rol.
* **Estudios de seguridad:** Para cargos críticos que impliquen acceso a información clasificada como pública reservada, se recomienda realizar estudios de seguridad física y psicológica.
* **Firma de acuerdos de confidencialidad:** Antes de iniciar actividades, todos los candidatos y contratistas deben firmar acuerdos de confidencialidad que se extienden a proveedores críticos con acceso a información reservada.
* **Definición de perfiles:** Cada puesto contará con un perfil documentado que especifique roles, responsabilidades y requisitos de acceso a la información, establecidos en colaboración con las direcciones y Talento Humano.
* **Contrataciones mediante terceros:** Cuando la selección sea realizada por terceros, los contratos incluirán cláusulas de manejo de datos personales, Seguridad de la Información y continuidad del negocio.
* **Almacenamiento de documentos:** La documentación recolectada será almacenada de forma segura, respetando la confidencialidad, integridad y disponibilidad de la información conforme a las normativas legales vigentes.
  1. **Durante la vinculación**
* **Inducción y capacitación:** Los nuevos empleados recibirán inducción dentro de los 30 días posteriores a su ingreso. Esta incluirá formación sobre Seguridad de la Información, privacidad de datos y procedimientos establecidos por el SGSI.
* **Compromiso con la seguridad:** Todos los colaboradores deberán aceptar las políticas, términos y condiciones relativas a la Seguridad de la Información y el manejo de datos personales, comprometiéndose a cumplirlas.
* **Asignación de activos y responsabilidades:** Se formalizará la entrega de activos y la asignación de responsabilidades, asegurando que cada colaborador proteja los recursos bajo su cargo.
* **Cultura de seguridad:** El Ministerio fomentará una cultura de seguridad basada en riesgos, donde los colaboradores sean responsables de reportar incidentes y seguir los procedimientos establecidos.
  1. **Terminación o cambio de labores**
* **Revocación de accesos:** Se coordinará la eliminación o modificación de derechos de acceso a sistemas e instalaciones para colaboradores que finalicen o cambien su relación laboral.
* **Devolución de activos:** Los activos asignados, físicos o digitales, serán devueltos y verificados para garantizar que no contengan información confidencial.
* **Transferencia de conocimiento:** Los colaboradores con conocimientos esenciales para la operación transferirán esta información a otros mediante procedimientos documentados.
* **Acuerdos de confidencialidad continuos:** Los acuerdos de confidencialidad seguirán vigentes incluso después de la finalización del contrato, dependiendo de la criticidad de la información manejada.
  1. **Procesos disciplinarios**
* **Sanciones por incumplimientos:** Las violaciones a las políticas de Seguridad de la Información serán tratadas mediante procesos disciplinarios formales, conforme a las normativas vigentes.
* **Evaluación de gravedad:** Las sanciones considerarán factores como la naturaleza de la violación, el impacto en los activos y el historial del infractor.
* **Procedimiento justo:** Todo proceso disciplinario será llevado a cabo con imparcialidad, garantizando un análisis exhaustivo de los hechos antes de tomar acciones.
  1. **Capacitación y concienciación en Seguridad de la Información**
* **Programas anuales:** El Ministerio desarrollará programas anuales de capacitación y sensibilización dirigidos a todas las partes interesadas con acceso a la información institucional.
* **Actualización de políticas:** Las actualizaciones en las políticas de Seguridad de la Información serán comunicadas de manera oportuna y reforzadas mediante procesos de sensibilización.
* **Evaluaciones periódicas:** Se realizarán evaluaciones para medir el nivel de comprensión y cumplimiento de las políticas entre los colaboradores.

**Alcance/aplicabilidad**

Esta política aplica a todos los empleados, contratistas y colaboradores del Ministerio de Minas y Energía, así como a terceros que interactúen con los activos de información de la Entidad.

**Nivel de cumplimiento de la política**

El cumplimiento del 100% de esta política es obligatorio para todos los involucrados. Auditorías internas y revisiones garantizarán la adherencia a los lineamientos establecidos.

**Excepciones a la política**

Cualquier solicitud de excepción deberá ser documentada, aprobada por el Oficial de Seguridad de la Información y revisada por la Mesa de Seguridad y Privacidad de la Información.

**Revisiones**

Esta política será revisada anualmente o cuando se presenten cambios significativos en el SGSI, MSPI, o en las condiciones internas o externas de la Entidad. Estas revisiones asegurarán su vigencia y alineación con los objetivos estratégicos del Ministerio.

### 7.2.9 Política de gestión y uso aceptable de activos

**Objetivo de la política**

Garantizar la protección, clasificación, inventario y uso adecuado de los activos de información del Ministerio de Minas y Energía, asegurando su disponibilidad, integridad, confidencialidad y trazabilidad. Además, fomentar una cultura de responsabilidad en el manejo de estos activos para minimizar riesgos y cumplir con las normativas aplicables.

La política de gestión y uso aceptable de activos del Ministerio de Minas y Energía establece:

Los activos de información involucrados en todos los procesos de la Entidad son propiedad del Ministerio de Minas y Energía y se proporcionan a las partes interesadas para cumplir con el propósito de la función pública.

Las partes interesadas son responsables de un adecuado y racional uso de los activos de información que se utilizan en los procesos del Ministerio de Minas y Energía; es decir, no se pueden usar para propósitos ni con configuraciones diferentes a las que fueron definidas por el Ministerio de Minas y Energía.

Los activos de información gestionados en todos los procesos del Ministerio de Minas y Energía deben cumplir con lo siguiente:

1. Seguir las políticas y procedimientos establecidos para la identificación y clasificación de activos, usos aceptables y entrega y devolución de activos.
2. Asignar un responsable del activo de información, quien debe ser el líder funcional y garantizar que dicho responsable esté capacitado en las normativas aplicables a la gestión de activos.
3. Mantener el inventario de activos actualizado y documentado en un sistema centralizado que permita su consulta y seguimiento.
4. Clasificar y proteger el activo de información de acuerdo con su valoración y categorías definidas en la normativa interna y legal.
5. Determinar, según la clasificación de los activos y mecanismos de protección, a quién se le permite el manejo de la información, el nivel de acceso y los procedimientos seguros para su adecuado tratamiento, el cual debe estar documentado en un procedimiento formal.
6. Realizar la clasificación de los activos según el tipo de activo (hardware, software, servicio, personas, etc.), revisándola periódicamente o cuando se presenten cambios que puedan afectarla.
7. Garantizar que los activos de información que contienen datos personales cumplan con la Ley 1581 de 2012 y las regulaciones complementarias.
8. Asegurar que las partes interesadas no compartan contraseñas ni permitan el acceso no autorizado a las cuentas otorgadas para utilizar los servicios brindados por la Entidad, siendo responsables por el manejo adecuado de la información y las acciones derivadas de su mal uso.
9. Implementar medidas adecuadas y fomentar una cultura para reportar cualquier anomalía identificada al oficial de seguridad de la información, según los procedimientos establecidos, con el fin de gestionar los riesgos e incidentes de seguridad.
10. Establecer que los datos de acceso son elementos personales e intransferibles, asumiendo las partes interesadas la responsabilidad sobre su uso.
11. Respaldar la información del Ministerio de Minas y Energía de forma frecuente y conforme a las políticas del SGSI, asegurando su almacenamiento en lugares adecuados para garantizar su recuperación en caso de desastres o incidentes.
12. Sancionar la copia, sustracción, daño intencional o utilización de los activos para fines distintos a las labores propias de la Entidad, conforme a la legislación vigente.
13. Asegurar que todos los activos sean revisados y auditados periódicamente para detectar posibles vulnerabilidades o desviaciones en su gestión.

**Inventario de activos:** Para proteger los activos de la Entidad, se debe elaborar y mantener un inventario de activos identificando propietarios y custodios designados:

1. Los activos de información serán claramente identificados y documentados con su nivel de importancia para el Ministerio de Minas y Energía, basado en la valoración del activo según el tipo de información que almacena, procesa o transmite.
2. La identificación de los activos incluirá elementos como tipo de activo, clasificación de la información y ubicación, considerando también su ciclo de vida.
3. Se debe contar con un procedimiento o instrucciones para la actualización del inventario de activos.
4. Se debe mantener un inventario de bases de datos con información personal, indicando lugares de almacenamiento, categoría y responsable de su legalidad, finalidad y protección.
5. Incorporar mecanismos tecnológicos que permitan rastrear y auditar los movimientos y cambios en el inventario de activos.

**Propietarios de los activos de información:**

1. Los propietarios de los activos son responsables de establecer y revisar periódicamente las restricciones y privilegios de acceso lógico y físico de proveedores, contratistas y usuarios.
2. Validar que los activos a su cargo cuenten con los controles requeridos para preservar los objetivos de legalidad, finalidad, integridad, confidencialidad y disponibilidad.
3. Actualizar periódicamente la valoración e información de los activos a su cargo, comprobando las necesidades de control.
4. Realizar capacitaciones periódicas sobre las responsabilidades y normativas asociadas a la gestión de activos.

**Alcance/aplicabilidad**

Esta política aplica a toda la Entidad, los usuarios y colaboradores del Ministerio de Minas y Energía, así como a la ciudadanía en general que tenga relación con los activos de información de la Entidad. El seguimiento y control del inventario consolidado de activos es responsabilidad del Grupo de Relacionamiento con el Ciudadano y Gestión de la Información.

**Nivel de cumplimiento de la política**

Todas las personas cubiertas por el alcance y aplicabilidad deben cumplir al 100% esta política.

**Excepciones a la política**

Cualquier modificación a la presente política debe ser escalada al oficial de seguridad de la información o quien haga sus veces, y revisada por la mesa de seguridad y privacidad de la información.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en el SGSI, SGCN, MSPI, partes interesadas o condiciones internas de la Entidad.

### 7.2.10 Política de uso aceptable de activos de información

**Objetivo de la política**

Garantizar la identificación, documentación e implementación de reglas claras para el uso aceptable de la información y de los activos asociados con información e instalaciones de procesamiento, asegurando el cumplimiento de los principios de seguridad, legalidad y buen manejo de los recursos del Ministerio de Minas y Energía.

La política de uso aceptable de activos establece:

Los empleados y usuarios de partes externas que utilizan activos del Ministerio de Minas y Energía o tienen acceso a ellos deben tomar conciencia de los requisitos de seguridad de la información relacionados con los activos, instalaciones y recursos de procesamiento de información. Son responsables del uso adecuado de cualquier recurso de procesamiento y de las acciones ejecutadas bajo su responsabilidad.

Todo uso de un activo de información de propiedad de la Entidad estará sujeto a las reglas de configuración, uso seguro y aceptable, tanto del activo como de la información que procese, transporte o almacene. Cualquier uso no autorizado será considerado un incumplimiento de las políticas establecidas y tendrá las sanciones correspondientes.

El Ministerio se reserva el derecho de realizar auditorías, revisiones periódicas y otros procedimientos necesarios para asegurar su cumplimiento. Para garantizar el buen uso de los activos de información y servicios, se debe conocer y aplicar los manuales e instructivos de las herramientas tecnológicas de la Entidad.

Esta política incluye los cambios requeridos en activos o entornos de trabajo que se utilizan dentro del flujo de desarrollo y adquisición de software y actividades de la Entidad. Cualquier cambio o modificación debe seguir el procedimiento de control de cambios establecido para determinar los riesgos potenciales de las modificaciones.

**En cuanto a uso aceptable, se establece:**

1. Los activos de información utilizados por los empleados o por personal externo deben emplearse exclusivamente para los fines, actividades y entornos de trabajo establecidos por la Entidad. Cualquier uso no autorizado está prohibido.
2. Las partes interesadas no deben compartir contraseñas ni permitir el acceso no autorizado a las cuentas otorgadas para utilizar los servicios del Ministerio, siendo responsables del manejo adecuado de la información y de las acciones derivadas de su mal uso.
3. Los datos de acceso son personales e intransferibles. Las partes interesadas asumen la responsabilidad sobre su uso adecuado o indebido.
4. La información del Ministerio debe ser respaldada periódicamente, conforme a las políticas validadas del SGSI y el MSPI, bajo la supervisión del oficial de seguridad de la información. El almacenamiento debe realizarse en lugares adecuados que garanticen su recuperación en caso de incidentes.
5. Para realizar copias de respaldo de archivos personales o información pública, se debe solicitar autorización al líder del proceso correspondiente y notificar al oficial de seguridad de la información.
6. La copia, sustracción, daño intencional o utilización de activos para fines ajenos a las labores de la Entidad será sancionada conforme a las leyes vigentes.
7. El acceso a información confidencial (uso interno, restringido o reservado) solo estará permitido a personas autorizadas por el propietario del activo.
8. Los repositorios de información deben estar custodiados y la información clasificada conforme a los niveles establecidos por el Ministerio.
9. Los colaboradores deben etiquetar la información según los niveles de clasificación definidos para proteger los activos de información a su cargo.

**En cuanto a la devolución de activos de información:**

1. Todos los funcionarios y usuarios externos deben devolver los activos de la Entidad a su cargo al finalizar su relación laboral o contractual o al cambiar sus funciones.
2. El proceso de terminación debe formalizarse, incluyendo la devolución de activos físicos y electrónicos entregados previamente.
3. En caso de que un empleado o contratista utilice su propio equipo personal, se deben implementar procedimientos que aseguren la transferencia y eliminación segura de la información del Ministerio almacenada en estos dispositivos.
4. Si el usuario posee conocimientos clave para la operación de la Entidad, esta información debe documentarse y transferirse al Ministerio.
5. Durante el período de notificación de terminación, el Ministerio debe supervisar que no se realicen copias no autorizadas de información confidencial o crítica.

**Alcance/aplicabilidad**

Esta política aplica a toda la Entidad, los usuarios y colaboradores del Ministerio de Minas y Energía, así como a la ciudadanía en general que tenga relación con los activos de información de la Entidad. El seguimiento y control del inventario consolidado de activos es responsabilidad del Grupo de Relacionamiento con el Ciudadano y Gestión de la Información.

**Nivel de cumplimiento de la política**

Todas las personas cubiertas por el alcance y aplicabilidad deben cumplir al 100% esta política.

**Excepciones a la política**

Cualquier modificación a la presente política debe ser escalada al oficial de seguridad de la información y revisada por la mesa de seguridad y privacidad de la información.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en el SGSI, SGCN, MSPI, partes interesadas o condiciones internas de la Entidad.

### 7.2.11 Política para clasificación de la información

**Objetivo de la política**

Garantizar que la información reciba un nivel apropiado de protección, de acuerdo con su importancia para el Ministerio de Minas y Energía, y asegurar su gestión alineada a las normativas legales y mejores prácticas en seguridad de la información.

El Ministerio de Minas y Energía establece la clasificación de la información a su cargo, alineada con:

* Ley 594 de 2000 (Ley General de Archivos).
* Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional).
* Ley 1581 de 2012 (Ley de Protección de Datos Personales).
* Decretos reglamentarios y normas complementarias aplicables.

**Criterios de clasificación de información:**

Los criterios para asignar la clasificación de la información están definidos por:

1. Cumplimiento regulatorio según las leyes mencionadas.
2. Impacto potencial de su divulgación en derechos individuales o intereses públicos.
3. Indicaciones de las normativas aplicables, como los artículos 18 y 19 de la Ley 1712 de 2014.

Toda la información bajo la custodia o control del Ministerio es considerada inicialmente pública, salvo que cumpla los criterios establecidos para ser clasificada como confidencial o reservada, descritos a continuación:

1. **Información pública:** Generada o controlada por el Ministerio, disponible para la ciudadanía en general. Ejemplos: planes de adquisiciones, rendición de cuentas, procedimientos de atención a la ciudadanía.
2. **Información clasificada o confidencial:** Aquella que, de divulgarse, podría causar daño a derechos individuales o afectar la intimidad y privacidad de personas. Ejemplos: liquidación de nóminas, secretos comerciales, quejas y reclamos.
3. **Información reservada:** Exceptuada de acceso por daño a intereses públicos o por seguridad nacional. Ejemplos: investigaciones disciplinarias, ubicación de almacenamiento de combustibles. El tiempo máximo de reserva es de 15 años desde la creación del documento, según la Ley 1712 de 2014.

**Procedimiento de clasificación:**

1. Toda información debe ser clasificada por su propietario según los niveles definidos, considerando su criticidad, sensibilidad y normativas vigentes.
2. Los líderes de proceso son responsables de garantizar la clasificación y revisión anual de la información y activos involucrados.
3. El Comité de Seguridad y Privacidad de la Información debe socializar y garantizar el cumplimiento del procedimiento de clasificación.

**Etiquetado y manejo de información:**

1. Desarrollar procedimientos para el etiquetado de información en formatos físicos y electrónicos, asegurando su identificación clara.
2. Respetar los lineamientos para la colocación de etiquetas en función del tipo de medio.
3. Prohibir el acceso, copia y uso no autorizado de información clasificada como confidencial o reservada.
4. Garantizar que la información confidencial no sea enviada sin cifrado por redes de comunicación o como archivos adjuntos.
5. Establecer protecciones físicas y lógicas para repositorios de información clasificada, procesada o almacenada.
6. Auditar periódicamente los repositorios para prevenir copias no autorizadas.

**Responsabilidades de los propietarios de información:**

1. Monitorear y actualizar periódicamente la clasificación y tiempos de retención de la información a su cargo.
2. Garantizar que los usuarios respeten las etiquetas y niveles de clasificación asignados.
3. Documentar cualquier reclasificación requerida y coordinar con el área de seguridad de la información.

**Alcance/aplicabilidad**

Esta política aplica a toda la Entidad, usuarios y colaboradores del Ministerio de Minas y Energía, así como a la ciudadanía que interactúe con activos de información de la entidad.

**Nivel de cumplimiento de la política**

Todas las personas cubiertas por esta política deben cumplir al 100% con sus disposiciones.

**Excepciones a la política**

Cualquier excepción debe ser escalada al oficial de seguridad de la información y revisada por la mesa de seguridad y privacidad de la información.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en el SGSI, MSPI, normativas legales o necesidades internas de la Entidad.

### 7.2.12 Política de control de acceso

**Objetivo de la política**

Limitar el acceso a información y a instalaciones de procesamiento de información, estableciendo, documentando y revisando una política de control de acceso basada en los requisitos del Ministerio de Minas y Energía y los principios de seguridad de la información.

**Política general**

El Ministerio de Minas y Energía establece los siguientes principios para la gestión de accesos:

1. Limitar, bajo los principios de separación de deberes, los accesos a entornos o ambientes de trabajo, repositorios de información y activos de información para todos los usuarios, ya sean funcionarios o personal externo.
2. Aplicar la premisa: “En general, todo está prohibido, a menos que se permita expresamente”. Solo se concede acceso a la información requerida para cumplir con las funciones asignadas (principios de “necesidad de saber” y “uso mínimo”).
3. Los propietarios de los activos de información son responsables de implementar y gestionar el control de acceso sobre los activos a nivel físico y lógico.
4. La configuración de accesos debe realizarse en conjunto con los propietarios de los activos, el Grupo TIC y el área de seguridad de la información, teniendo en cuenta los riesgos asociados, la justificación de negocio y los criterios de separación de deberes.
5. Todo acceso configurado es de carácter personal e intransferible. Está prohibido compartir credenciales o utilizar accesos de otros usuarios.

**Lineamientos específicos para el cumplimiento de la política:**

1. **Validación y seguimiento:**
   * El oficial de seguridad de la información debe validar los accesos a nivel de red, instalaciones físicas, sistemas operativos, bases de datos y aplicaciones.
   * Implementar controles que limiten el acceso al mínimo requerido para el desempeño de roles o funciones.
   * Identificar de manera inequívoca a cada usuario y realizar seguimientos periódicos o aleatorios de sus actividades.
2. **Configuración de contraseñas seguras:**
   * Definir contraseñas con características de complejidad (longitud, combinación de caracteres) y establecer cambios periódicos cada 60 días.
   * Implementar bloqueo automático tras varios intentos fallidos y exigir cambio de contraseña en el primer inicio de sesión.
   * Registrar histórico de al menos seis contraseñas anteriores para evitar su reutilización.
3. **Acceso a redes y servicios:**
   * Los colaboradores deben utilizar los servicios de correo electrónico y navegación en internet exclusivamente para actividades laborales.
   * Implementar monitoreo y filtrado de navegación basado en perfiles laborales.
   * Restringir el uso de redes inalámbricas a aquellas configuradas con protocolos seguros y aprobadas por el Grupo TIC.
4. **Gestión de accesos privilegiados:**
   * Controlar los accesos de altos privilegios mediante autorización formal y revisión periódica por parte del área de seguridad de la información.
   * Mantener un registro detallado de usuarios con privilegios elevados y monitorear sus actividades.
   * Restringir la configuración de dispositivos y servicios de red a personal autorizado.
5. **Registro y cancelación de usuarios:**
   * Implementar un procedimiento para gestionar altas, modificaciones y bajas de usuarios en sistemas de información.
   * Bloquear de inmediato los accesos de usuarios que cambien de funciones, terminen contratos o sufran pérdida de credenciales.
   * Revisar periódicamente identificadores de usuario, eliminando cuentas redundantes o inactivas.
6. **Roles y responsabilidades:**
   * Cada dependencia del Ministerio debe definir los perfiles de usuario necesarios para sus procesos y validarlos con el oficial de seguridad de la información.
   * Los propietarios de los sistemas deben verificar y ratificar semestralmente las autorizaciones otorgadas a sus usuarios.

**Suministro y gestión de accesos:**

1. Los accesos no deben activarse antes de cumplir con el proceso de autorización establecido.
2. Adaptar o revocar derechos de acceso inmediatamente se cambien roles o se termine una relación contractual.
3. Establecer auditorías periódicas para evaluar la vigencia de los accesos y prevenir usos indebidos.
4. Documentar las solicitudes y aprobaciones de acceso en un registro centralizado.
5. Garantizar que las actividades de usuarios con accesos especiales sean trazables y supervisadas.

**Excepciones a la política**

Cualquier excepción a esta política debe ser autorizada por el oficial de seguridad de la información y revisada por la mesa de seguridad y privacidad de la información o quien haga sus veces.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los sistemas, normativas o estructuras organizacionales del Ministerio.

### 7.2.13 Política para gestión de autenticación secreta de usuarios o de contraseñas

**Objetivo de la política**

Garantizar la asignación, uso y protección de la información de autenticación secreta mediante un proceso de gestión formal, asegurando que solo el personal autorizado acceda a los recursos y sistemas del Ministerio de Minas y Energía.

**Política general**

El Ministerio de Minas y Energía implementa medidas para garantizar la seguridad en la gestión de contraseñas como medio de validación de identidad digital y control de acceso a los sistemas de información. Estas medidas incluyen:

1. **Asignación de contraseñas:**
   * Uso obligatorio de contraseñas individuales y no compartidas.
   * Prohibición del uso de cuentas genéricas o contraseñas comunes.
2. **Generación de contraseñas seguras:**
   * Contraseñas con una longitud mínima de 12 caracteres, que incluyan combinaciones de letras mayúsculas y minúsculas, números y caracteres especiales.
   * Evitar contraseñas basadas en información personal o fácilmente adivinable.
3. **Cambio y gestión de contraseñas:**
   * Cambio obligatorio al primer inicio de sesión.
   * Renovación periódica de contraseñas cada 60 días.
   * Almacenamiento seguro y prohibición de registrar contraseñas en medios no protegidos.
4. **Manejo de contraseñas predeterminadas:**
   * Cambiar inmediatamente las contraseñas predeterminadas de sistemas y dispositivos al momento de la instalación.
5. **Autenticación múltiple (MFA):**
   * Implementación de autenticación múltiple en entornos de redes públicas, combinando contraseñas con otros factores como biometría y tokens.
6. **Responsabilidades de los usuarios:**
   * Mantener la confidencialidad de sus credenciales.
   * Informar de inmediato cualquier sospecha de compromiso de contraseñas.
   * Cambiar las contraseñas de inmediato ante cualquier exposición no autorizada.

**Sistema de gestión de contraseñas:**

1. **Configuración y controles:**
   * Configurar sistemas para cumplir con los requisitos de complejidad y almacenamiento seguro de contraseñas.
   * Eliminar cuentas no utilizadas o inactivas por más de 60 días.
   * Impedir la reutilización de al menos las últimas 6 contraseñas.
2. **Procedimientos formales:**
   * Asegurar que los usuarios comprendan y acepten sus responsabilidades mediante la firma de declaraciones de cumplimiento.
   * Verificar que los niveles de acceso otorgados sean consistentes con las responsabilidades asignadas.
3. **Auditoría y monitoreo:**
   * Realizar auditorías periódicas para identificar y corregir posibles vulnerabilidades en la gestión de contraseñas.
   * Mantener registros detallados de las contraseñas asignadas y cambios realizados.
4. **Educación y concienciación:**
   * Implementar programas de capacitación para educar a los usuarios sobre las mejores prácticas en seguridad de contraseñas.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, usuarios y colaboradores del Ministerio de Minas y Energía, así como a la ciudadanía que interactúe con los activos de información del Ministerio.

**Nivel de cumplimiento de la política**

Todas las personas cubiertas por esta política deben cumplir al 100% sus disposiciones.

**Excepciones a la política**

Cualquier excepción debe ser justificada y aprobada por el oficial de seguridad de la información y revisada por la mesa de seguridad y privacidad de la información.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los sistemas, normativas o necesidades de seguridad del Ministerio.

### 7.2.14 Política para uso de controles criptográficos

**Objetivo de la política**

Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información, cumpliendo con los más altos estándares de seguridad en el manejo de datos sensibles y confidenciales.

**Uso de controles criptográficos:**

Los controles criptográficos se implementan para cumplir con los siguientes propósitos:

1. **Confidencialidad:** Aplicación de técnicas de cifrado para asegurar que la información sensible, ya sea almacenada o transmitida, no sea accesible a personas no autorizadas.
2. **Integridad y autenticidad:** Uso de firmas digitales y códigos de autenticación de mensajes para garantizar que la información no haya sido alterada y que su origen sea verificable.
3. **No repudio:** Uso de métodos criptográficos para proporcionar evidencia innegable de que un evento o acción ha ocurrido, como en contratos digitales o transacciones.
4. **Autenticación:** Verificación de identidades y entidades a través de técnicas criptográficas, asegurando que solo usuarios autorizados accedan a sistemas y recursos.

**Protección de información sensible y confidencial:**

El Ministerio de Minas y Energía protegerá la siguiente información utilizando controles criptográficos:

* Bases de datos que contengan información sensible, incluyendo registros de usuarios.
* Correos electrónicos que contengan datos confidenciales o estratégicos.
* Información protegida por leyes y regulaciones, como datos personales bajo la Ley 1581 de 2012.
* Copias de seguridad (backups), tanto locales como en la nube.
* Datos almacenados en dispositivos móviles o removibles, como discos duros externos y USBs.
* Credenciales de acceso y datos financieros que requieran protección adicional.

**Técnicas y análisis previos:**

1. **Análisis de riesgos:** Antes de implementar controles criptográficos, se debe identificar la información crítica y evaluar los riesgos asociados.
2. **Valoración del uso de firma digital:** Determinar escenarios donde sea necesario autenticar documentos, garantizar su integridad o asegurar el no repudio.
3. **Definición de niveles de protección:** Basado en el análisis, establecer qué datos requieren cifrado y bajo qué condiciones se aplicarán estos controles.

**Protocolos seguros en comunicaciones:**

Para proteger las comunicaciones digitales, el Ministerio implementará:

* VPNs cifradas para teletrabajadores y acceso remoto seguro.
* Certificados web (SSL/TLS) actualizados para todos los servicios web oficiales.
* Envío de información sensible exclusivamente a través de canales cifrados.

**Declaración de compromiso:**

El Ministerio se compromete a garantizar el uso adecuado de técnicas criptográficas en los siguientes casos:

1. **Protección de claves de acceso:** Incluyendo credenciales utilizadas para sistemas, datos y servicios.
2. **Transmisión de información clasificada:** Cuando se utilicen redes públicas o servicios externos.
3. **Almacenamiento seguro de datos confidenciales:** Aplicable a medios removibles, dispositivos móviles y copias de seguridad.
4. **Administración de llaves criptográficas:** Implementando un sistema que permita su recuperación segura en caso de pérdida o compromiso.
5. **Controles sobre software malicioso:** Permitiendo el descifrado temporal para análisis y escaneo.

**Principios para la implementación:**

1. **Identificación de datos a cifrar:** Basado en la política de clasificación de la información, incluyendo datos sensibles, credenciales de autenticación y transferencias en redes inseguras.
2. **Determinación de uso de firma electrónica:** En trámites oficiales, emisión de facturas y transacciones que requieran autenticidad y no repudio.
3. **Selección de proveedores de certificados:** Garantizando cumplimiento legal, validez, y opciones de revocación.
4. **Certificados web y cifrado de servicios en la nube:** Asegurando la confidencialidad e integridad en plataformas externas.

**Protección de datos en servicios externos:**

* Cifrado de datos antes de transferirlos a servicios externos o proveedores.
* Uso de canales seguros, como VPN, para intercambios de información.
* Verificación de que los proveedores cumplen con estándares internacionales de seguridad, como PCI-DSS para pasarelas de pago.

**Desarrollos de aplicaciones:**

* Incorporar privacidad por diseño y por defecto en todos los desarrollos.
* Cifrar contraseñas y otros datos críticos en bases de datos de aplicaciones.
* Establecer controles para garantizar que el diseño del software respete la confidencialidad y la integridad de los datos procesados.

**VPN y conexiones externas:**

* Establecer canales VPN cifrados para accesos remotos.
* Configurar redes WiFi con estándares como WPA3, cambiando claves predeterminadas para evitar vulnerabilidades.

**Uso de algoritmos criptográficos:**

* Utilizar algoritmos actualizados y ampliamente evaluados.
* Priorizar cifrados de estándares abiertos y de especificaciones públicas, como AES y RSA.

**Aplicaciones autorizadas:**

El Ministerio define aplicaciones para los siguientes usos:

* Cifrado de discos locales y extraíbles.
* Protección de correos y backups.
* Cifrado de archivos, carpetas y repositorios.
* Herramientas para garantizar la privacidad de datos en dispositivos móviles.

**Protocolos seguros:**

* **SSH:** Acceso remoto seguro a servidores y dispositivos.
* **SFTP/FTPS:** Transferencia cifrada de datos.
* **HTTPS:** Comunicaciones seguras en servicios web.

**Gestión de llaves y certificados criptográficos:**

1. **Generación y entrega formal:** Ante cambios organizacionales, garantizar la actualización o revocación de llaves.
2. **Auditorías anuales:** Revisar el manejo, uso y custodia de llaves y certificados.
3. **Documentación detallada:** Incluir manuales para la implementación y renovación de certificados.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, los usuarios, colaboradores del Ministerio de Minas y Energía, y la ciudadanía en general que interactúe con los activos de información del Ministerio.

**Nivel de cumplimiento de la política**

Todas las personas cubiertas por esta política deben cumplir al 100% sus disposiciones.

**Excepciones a la política**

Cualquier excepción debe ser justificada y aprobada por el oficial de seguridad de la información y revisada por la mesa de continuidad y gestión del cambio.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los sistemas, normativas o necesidades de seguridad del Ministerio.

### 7.2.15 Política para gestión de llaves criptográficas

**Objetivo de la política**

Asegurar la implementación, uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo, garantizando su eficacia y seguridad en las operaciones del Ministerio de Minas y Energía.

**Gestión de llaves criptográficas:**

El Ministerio de Minas y Energía establece procedimientos claros y rigurosos para la gestión de llaves criptográficas, abarcando desde su generación hasta su destrucción. Estas llaves son fundamentales para mantener la confidencialidad, integridad y autenticidad de la información procesada por la Entidad.

Las llaves criptográficas deben protegerse contra cualquier riesgo de modificación, pérdida, divulgación o uso indebido. Esto incluye su generación en equipos protegidos por controles físicos y técnicos, alineados con estándares internacionales reconocidos. Cada llave generada debe contar con identificadores únicos que permitan su trazabilidad a lo largo de su ciclo de vida.

Los procedimientos internos de cada dependencia deben definir, de manera específica, los lineamientos para la generación, almacenamiento, distribución y eventual eliminación de las llaves criptográficas, adaptándose a las necesidades operativas de cada área. Estos procedimientos incluirán detalles como la identificación de propietarios, fechas de emisión y revocación, así como los propósitos y limitaciones de cada llave.

El uso de certificados de llaves públicas emitidos por autoridades certificadoras acreditadas es esencial para garantizar la autenticidad de las llaves públicas. Este proceso debe estar respaldado por contratos claros con proveedores externos, que especifiquen responsabilidades, confiabilidad de los servicios y tiempos de respuesta ante incidentes.

**Principios de uso:**

La gestión de llaves criptográficas debe incluir controles para asegurar su disponibilidad únicamente durante el período necesario. Esto implica la definición de fechas de activación y desactivación, así como la revocación o reemplazo inmediato en caso de compromiso de su seguridad. Asimismo, se debe implementar un sistema robusto para la recuperación de llaves en caso de pérdida o daño, asegurando que los datos asociados no queden inaccesibles.

Los responsables de estas actividades, principalmente el Grupo TIC y el oficial de seguridad de la información, deben garantizar que todos los procedimientos asociados a la gestión de llaves sean documentados y probados regularmente. Las actividades de emergencia ante fallos o desastres deben estar claramente establecidas y ser objeto de simulaciones periódicas para validar su eficacia.

**Implementación de un sistema de gestión de llaves:**

El sistema debe contemplar normas y procedimientos para:

* Generación y distribución segura de llaves para diferentes sistemas y aplicaciones.
* Almacenamiento en entornos protegidos, con acceso restringido a usuarios autorizados.
* Revisión periódica de las llaves para garantizar su vigencia y adecuación a las necesidades de seguridad.
* Revocación y eliminación segura de llaves comprometidas o que ya no sean necesarias.
* Creación de copias de respaldo que permitan su recuperación en caso de contingencias.

**Auditoría y monitoreo:**

Todas las actividades relacionadas con la gestión de llaves deben ser registradas y auditadas al menos una vez al año. Esto incluye la revisión de los procedimientos y controles implementados para garantizar que se mantengan alineados con las mejores prácticas y las normativas vigentes. Además, los manuales operativos asociados a la implementación y gestión de llaves criptográficas deben mantenerse actualizados y disponibles para su consulta por los responsables designados.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, sus usuarios y colaboradores, así como a cualquier parte interesada que interactúe con los activos de información del Ministerio de Minas y Energía.

**Nivel de cumplimiento de la política**

Todas las personas cubiertas por esta política deben garantizar el cumplimiento del 100% de sus disposiciones, sin excepción.

**Excepciones a la política**

Cualquier excepción debe ser justificada y aprobada por el oficial de seguridad de la información y revisada por la mesa de continuidad y gestión del cambio.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los sistemas, normativas o necesidades de seguridad del Ministerio.

### 7.2.16 Política de seguridad física y trabajo en áreas seguras

**Objetivo de la política**

Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información del Ministerio de Minas y Energía, asegurando un entorno seguro que respalde la integridad, confidencialidad y disponibilidad de los activos críticos de información.

**Política general de seguridad física:**

El Ministerio implementa medidas de seguridad física integrales para proteger sus instalaciones, activos de información y sistemas críticos. Estas medidas incluyen controles de acceso, vigilancia, mantenimiento preventivo y respuesta ante emergencias, considerando tanto amenazas internas como externas.

**Controles físicos y gestión de accesos:**

1. **Ingreso y egreso controlado:**
   * Los accesos deben registrarse, y todo personal y visitantes deben portar identificaciones visibles mientras permanezcan en las instalaciones.
   * Los visitantes requieren autorización previa y deben ser acompañados por un funcionario designado durante toda su visita.
2. **Perímetros de seguridad:**
   * Definir barreras físicas como muros, puertas controladas por dispositivos de autenticación y sistemas de vigilancia que delimiten las áreas críticas.
   * Estas áreas deben estar señalizadas visiblemente y protegidas contra acceso no autorizado.
   * Implementar puertas contra incendios con sistemas de alarma y mecanismos de cierre automático.
3. **Clasificación de zonas de acceso:**
   * **Libre acceso:** Áreas generales como recepción, disponibles para visitantes controlados.
   * **Acceso controlado:** Espacios que requieren autorización previa, gestionada mediante sistemas electrónicos y vigilancia.
   * **Acceso restringido:** Áreas críticas con información sensible, accesibles solo para personal autorizado bajo estrictas medidas de seguridad.

**Seguridad física en oficinas y recintos:**

1. **Políticas generales:**
   * Restringir el acceso del público general y de terceros no autorizados.
   * Guardar documentos confidenciales en gabinetes seguros cuando no estén en uso.
   * Cumplir con las normativas del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST).
2. **Protección de equipos tecnológicos:**
   * Evitar materiales combustibles en áreas con equipos tecnológicos.
   * Implementar detectores y extintores de incendios adecuados, probados cada seis meses.
   * Proteger el cableado estructurado contra interferencias, daño y manipulación.

**Gestión de áreas de carga y despacho:**

* Restringir el acceso solo a personal autorizado.
* Aislar físicamente estas zonas de las áreas de procesamiento de información.
* Inspeccionar minuciosamente todo material que ingrese o salga, verificando su conformidad con los estándares de gestión de activos.

**Protección de equipos y activos:**

1. **Condiciones ambientales:**
   * Centros de cómputo y áreas críticas deben contar con controles de temperatura, humedad y suministro eléctrico continuo.
   * Implementar sistemas de respaldo como UPS y plantas eléctricas.
2. **Disposición y uso de equipos:**
   * Ubicar estaciones de trabajo para evitar el acceso visual de personas no autorizadas.
   * Proteger equipos contra amenazas físicas como fuego, agua y vandalismo.

**Trabajo en áreas seguras:**

1. **Acceso controlado:**
   * Prohibido el ingreso de dispositivos no autorizados como cámaras o teléfonos inteligentes, sin previa aprobación.
   * La ubicación y disposición de los sistemas de procesamiento de información son clasificadas y divulgadas solo a personal autorizado.
2. **Supervisión permanente:**
   * Las áreas seguras vacías deben permanecer cerradas y bajo monitoreo continuo mediante cámaras o sensores de movimiento.

**Gestión de equipos fuera de las instalaciones:**

1. **Medidas de seguridad:**
   * Aplicar cifrado de información en equipos utilizados fuera de las instalaciones.
   * Mantener registros detallados sobre la custodia y uso de activos.
2. **Responsabilidades del personal:**
   * Los funcionarios son responsables por pérdida, daño o robo de equipos cuando no cumplan con las medidas de seguridad definidas.

**Mantenimiento de equipos:**

1. **Mantenimiento preventivo y correctivo:**
   * Solo personal autorizado puede realizar estas actividades, registrándolas detalladamente.
   * Antes de intervenir un equipo, se debe garantizar el respaldo de la información crítica.
2. **Retiro de activos:**
   * Cualquier equipo retirado requiere autorización formal y registro completo.
   * Garantizar que la información sensible esté cifrada antes de retirar equipos de áreas críticas.

**Protección contra amenazas internas y externas:**

1. **Amenazas físicas:**
   * Mitigar riesgos como incendios, inundaciones y desastres naturales mediante evaluaciones anuales y controles adecuados.
2. **Amenazas lógicas:**
   * Proteger sistemas contra sabotaje, acceso remoto no autorizado y suplantación de identidad mediante controles robustos y análisis de riesgos periódicos.

**Seguridad del cableado estructurado:**

* Proteger el cableado contra daños, interceptaciones y manipulación.
* Separar rutas de cableado de energía y comunicaciones para evitar interferencias.
* Realizar inspecciones periódicas para detectar conexiones no autorizadas.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, los usuarios, colaboradores del Ministerio de Minas y Energía, y terceros que interactúen con sus activos e instalaciones.

**Nivel de cumplimiento de la política**

Todas las personas cubiertas por esta política deben cumplir al 100% sus disposiciones.

**Excepciones a la política**

Cualquier excepción debe ser aprobada por el oficial de seguridad de la información y revisada por la mesa de continuidad y gestión del cambio.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en las normativas, riesgos identificados o necesidades operativas.

### 7.2.17 Política de escritorio y pantalla limpia

**Objetivo de la política**

Garantizar la protección de la información confidencial y sensible del Ministerio de Minas y Energía mediante la adopción de una política de escritorio limpio para documentos físicos y medios de almacenamiento removibles, así como una política de pantalla limpia en los dispositivos de procesamiento de información.

**Pautas generales**

El Ministerio implementa y supervisa las mejores prácticas para la gestión y resguardo de información, promoviendo la organización y seguridad en los espacios de trabajo, tanto físicos como digitales. Estas prácticas buscan minimizar el riesgo de acceso no autorizado, pérdida, robo o daño a la información.

**Políticas específicas de escritorio limpio:**

1. **Conservación del entorno de trabajo:**
   * Los escritorios deben mantenerse libres de documentos, dispositivos de almacenamiento o cualquier elemento que contenga información confidencial o sensible cuando no estén en uso.
   * Los documentos confidenciales deben guardarse bajo llave en archivadores o gabinetes seguros al final de la jornada laboral o cuando el espacio de trabajo quede desocupado.
2. **Manejo de documentos impresos:**
   * Los documentos que contienen información confidencial deben ser retirados de inmediato de impresoras, fotocopiadoras o faxes.
   * Cualquier documento abandonado en estas estaciones será tratado como un incidente de seguridad y gestionado según los procedimientos establecidos.
   * Las copias innecesarias de documentos confidenciales deben destruirse de manera segura mediante triturado o métodos similares.
3. **Prohibición de almacenamiento indebido:**
   * No se permite guardar credenciales de acceso o información sensible en escritorios, cajones sin llave, ni en papeles visibles.
   * Los elementos de trabajo deben ser los estrictamente necesarios para la actividad laboral, evitando accesos directos a aplicativos o repositorios en escritorios.

**Políticas específicas de pantalla limpia:**

1. **Bloqueo de dispositivos:**
   * Los usuarios deben bloquear la pantalla de sus equipos mediante protectores de pantalla con contraseñas siempre que se ausenten de su estación de trabajo.
   * Si el sistema no cuenta con bloqueo automático, los usuarios deben reportarlo inmediatamente al Grupo TICS para su corrección.
2. **Cierre de sesiones:**
   * Se deben cerrar las sesiones activas en sistemas, aplicativos o plataformas cuando no estén en uso.
   * Está prohibido dejar dispositivos desatendidos sin activar las medidas de bloqueo adecuadas.

**Responsabilidades de las partes interesadas:**

1. **Cumplimiento de la política:**
   * Todos los usuarios son responsables de aplicar estas medidas y de informar cualquier anomalía que detecten en su entorno de trabajo.
   * El incumplimiento de estas disposiciones será tratado como una violación de las políticas de seguridad y podría conllevar sanciones disciplinarias.
2. **Gestión de incidentes:**
   * Cualquier acceso no autorizado a información debido a negligencia en la aplicación de esta política deberá ser reportado y tratado como incidente de seguridad.

**Controles adicionales:**

1. **Monitoreo y auditoría:**
   * Se realizarán auditorías periódicas para garantizar el cumplimiento de las políticas de escritorio y pantalla limpia.
   * El personal de seguridad podrá realizar revisiones aleatorias en las estaciones de trabajo para verificar la correcta implementación de estas políticas.
2. **Capacitación:**
   * Los usuarios recibirán capacitaciones regulares sobre la importancia de mantener un escritorio y pantalla limpia, así como las mejores prácticas para garantizar la seguridad de la información.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, los usuarios, colaboradores del Ministerio de Minas y Energía y a cualquier tercero que interactúe con los activos de información o espacios de trabajo del Ministerio.

**Nivel de cumplimiento de la política**

Todas las personas cubiertas por esta política deben cumplir estrictamente con sus disposiciones, garantizando un nivel de cumplimiento del 100%.

**Excepciones a la política**

Cualquier excepción debe ser autorizada por el Oficial de Seguridad de la Información y/o quien haga sus veces, y revisada por la mesa de seguridad y privacidad de la información.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los componentes del SGSI, en los procesos internos del Ministerio o en las partes interesadas que interactúan con la información.

### 7.2.18 Política para control de cambios

**Objetivo de la política**

Garantizar que los cambios en los procesos de negocio, instalaciones y sistemas de procesamiento de información que puedan afectar la seguridad de la información sean gestionados de manera controlada, minimizando riesgos, asegurando la continuidad operativa y protegiendo los activos de información del Ministerio de Minas y Energía.

**Política general**

El Ministerio de Minas y Energía adopta un enfoque integral para la gestión de cambios, garantizando que cada modificación sea evaluada, documentada y aprobada formalmente antes de su implementación. Este control se fundamenta en las mejores prácticas internacionales como ISO 20000 e ITIL, asegurando que los cambios contribuyan al cumplimiento de los objetivos estratégicos y operativos de la Entidad.

**Gestión de cambios**

El control de cambios es una disciplina esencial que abarca la identificación, evaluación, aprobación, implementación y monitoreo de modificaciones en sistemas, procesos y activos. Todo cambio debe ser gestionado de manera formal desde su concepción hasta su implementación, asegurando trazabilidad y cumplimiento normativo.

Para ello, el Ministerio ha constituido una Mesa de Trabajo de Cambios, compuesta por el Oficial de Seguridad de la Información, el Grupo TICS y representantes de los procesos involucrados. Este grupo es responsable de revisar cada solicitud de cambio, evaluar su impacto y autorizar su ejecución, asegurando que no se comprometan los niveles de seguridad ni la operatividad de los sistemas.

**Evaluación de riesgos y planificación:**

Antes de implementar un cambio, se debe realizar una evaluación exhaustiva de los riesgos asociados, considerando:

* Impactos potenciales en la seguridad de la información, disponibilidad de sistemas y cumplimiento normativo.
* Alteraciones en los flujos operativos y la continuidad de los servicios.
* Medidas de mitigación para prevenir o responder a posibles fallos durante o después del cambio.

Los cambios deben planificarse meticulosamente, incluyendo la definición de objetivos claros, asignación de responsabilidades, y creación de cronogramas que minimicen la afectación a las operaciones críticas.

**Documentación y trazabilidad:**

Cada cambio debe estar respaldado por una documentación completa que incluya:

* Descripción detallada del cambio.
* Justificación y objetivos.
* Evaluación de riesgos y medidas de mitigación.
* Plan de implementación, pruebas y validación.
* Resultados obtenidos y lecciones aprendidas.

Esta documentación debe integrarse en un registro centralizado, proporcionando trazabilidad y facilitando auditorías posteriores.

**Comunicación:**

Es esencial garantizar que todos los interesados estén informados sobre los cambios planificados. Esto incluye:

* Notificación previa a las dependencias y usuarios afectados.
* Divulgación de los procedimientos de recuperación en caso de fallos.
* Publicación de informes que detallen el alcance y resultados de los cambios.

**Auditoría y monitoreo:**

El registro de auditoría para cada cambio implementado debe mantenerse actualizado, permitiendo:

* Revisiones periódicas de cumplimiento con los procedimientos establecidos.
* Identificación de áreas de mejora en la gestión de cambios.
* Respuesta eficaz a incidentes derivados de modificaciones en los sistemas.

**Gestión de capacidad:**

El Ministerio, a través del Grupo TICS, evalúa constantemente las necesidades de capacidad de procesamiento y almacenamiento, garantizando que los recursos tecnológicos sean adecuados y estén alineados con las demandas actuales y futuras. Esto incluye:

* Proyecciones basadas en análisis de tendencias operativas.
* Implementación de herramientas para monitorear el rendimiento de los sistemas.
* Ajustes proactivos para prevenir cuellos de botella en la infraestructura tecnológica.

**Separación de ambientes:**

La integridad de los sistemas de información se refuerza mediante la segregación de los ambientes de desarrollo, pruebas y producción. Esto incluye:

* Definición de roles y responsabilidades para cada etapa del ciclo de vida de los sistemas.
* Implementación de controles que restrinjan el acceso a datos sensibles en entornos de pruebas.
* Prohibición de pruebas o desarrollos en ambientes de producción, salvo en casos excepcionales y autorizados.
* Monitoreo periódico de las versiones instaladas para garantizar consistencia y prevenir errores.

**Restricciones y autorizaciones**

Cualquier copia de información clasificada desde producción a entornos de prueba debe ser autorizada por el propietario de la información, el Coordinador del Grupo TICS y el Oficial de Seguridad de la Información. Estas copias deben eliminarse de forma segura tras su uso.

**Alcance/Aplicabilidad**

Esta política aplica a todos los usuarios, colaboradores y terceros que interactúen con los sistemas, procesos y activos de información del Ministerio de Minas y Energía.

**Nivel de cumplimiento de la política**

Todas las personas cubiertas por esta política deben cumplir rigurosamente con sus disposiciones. El incumplimiento será tratado como una violación de las políticas de seguridad y gestionado conforme a los procedimientos disciplinarios de la Entidad.

**Excepciones**

Cualquier excepción a esta política debe ser debidamente justificada, aprobada por el Oficial de Seguridad de la Información y revisada por la Mesa de Continuidad y Gestión del Cambio.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los sistemas, procesos o normativas aplicables, garantizando su relevancia y efectividad en el contexto operativo del Ministerio.

### 7.2.19 Política de protección contra códigos maliciosos

**Objetivo de la política**

Asegurar que la información y las instalaciones de procesamiento de información del Ministerio de Minas y Energía estén protegidas contra amenazas asociadas a códigos maliciosos, garantizando la continuidad operativa y la integridad de los sistemas.

**Política general**

El Ministerio implementa controles proactivos y reactivos para prevenir, detectar y mitigar los efectos de códigos maliciosos. Estos controles se combinan con programas de concienciación dirigidos a los usuarios, promoviendo buenas prácticas en la manipulación de información y el uso de sistemas tecnológicos.

**Controles y medidas de protección:**

1. **Prohibición de software no autorizado:**
   * Está prohibido instalar o utilizar software no autorizado en equipos del Ministerio. Cualquier software debe ser aprobado y gestionado por el Grupo TICS, garantizando su legitimidad y seguridad.
2. **Procedimientos de manejo seguro de archivos y software:**
   * Se redactarán y mantendrán procedimientos claros para la obtención, manipulación y uso de archivos y software provenientes de fuentes externas o no confiables.
   * Estos procedimientos incluirán medidas específicas para prevenir riesgos asociados a descargas desde internet, correos electrónicos y medios extraíbles.
3. **Instalación y actualización de software de protección:**
   * Se instalarán soluciones de detección y eliminación de malware en todos los sistemas y equipos del Ministerio.
   * Estas herramientas deben mantenerse actualizadas regularmente para responder eficazmente a nuevas amenazas.
4. **Gestión de actualizaciones de seguridad:**
   * Los sistemas deben mantenerse actualizados con los parches de seguridad más recientes.
   * Las actualizaciones críticas serán probadas previamente en entornos controlados para evaluar su impacto antes de su implementación generalizada.
5. **Revisión y auditoría de contenido:**
   * Se revisará periódicamente el contenido de software y datos almacenados en los equipos de procesamiento, investigando posibles archivos no aprobados o modificaciones no autorizadas.
   * Estas auditorías garantizarán que solo se utilice software legítimo y alineado con los objetivos del Ministerio.
6. **Verificación de medios externos:**
   * Antes de utilizar medios electrónicos externos, como USBs o discos duros, se debe verificar la presencia de malware utilizando las herramientas de detección del Ministerio.
   * Se aplicarán políticas restrictivas para limitar el uso de dispositivos de almacenamiento removibles no autorizados.

**Concienciación y formación:**

El Ministerio implementará programas regulares de capacitación para todos los usuarios, abordando temas como:

* Identificación y prevención de ataques basados en ingeniería social, como phishing.
* Buenas prácticas para evitar la propagación de malware.
* Responsabilidades individuales en la protección de los activos de información del Ministerio.

**Monitoreo y respuesta:**

El Grupo TICS, en coordinación con el Oficial de Seguridad de la Información, implementará sistemas de monitoreo continuo para detectar actividades sospechosas asociadas a códigos maliciosos. Estos sistemas incluirán:

* Monitoreo en tiempo real del tráfico de red y actividades inusuales en los sistemas.
* Alertas automatizadas para incidentes relacionados con malware.
* Procedimientos de respuesta rápida que incluyan aislamiento de sistemas comprometidos y restauración desde copias de seguridad seguras.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, incluyendo a los usuarios, colaboradores y terceros que utilicen o interactúen con los activos de información del Ministerio de Minas y Energía.

**Nivel de cumplimiento de la política**

El cumplimiento es obligatorio para todas las personas cubiertas por esta política. Las violaciones serán gestionadas según los procedimientos disciplinarios establecidos por el Ministerio.

**Excepciones**

Cualquier excepción debe ser justificada, aprobada por el Oficial de Seguridad de la Información y revisada por la mesa de seguridad y privacidad de la información.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los sistemas, amenazas identificadas o necesidades operativas del Ministerio, asegurando su relevancia y efectividad en el contexto actual.

### 7.2.20 Política de respaldo de información

**Objetivo de la política**

Asegurar la disponibilidad y restauración de la información crítica, software e imágenes de sistemas mediante la implementación de copias de respaldo confiables, almacenadas de forma segura, y la realización de pruebas regulares para garantizar su eficacia.

**Política general**

El Ministerio de Minas y Energía garantiza la generación continua de copias de respaldo de su información crítica. Estas copias serán almacenadas en medios seguros, tanto internos como externos, bajo estrictos controles de seguridad física, lógica y ambiental. Se implementarán procedimientos claros para realizar, verificar y restaurar las copias de respaldo, minimizando el impacto de posibles desastres o contingencias.

**Almacenamiento y clasificación de respaldos:**

1. **Ubicación interna y externa:**
   * Las copias de respaldo se almacenarán en sitios internos y externos según la clasificación de la información.
   * El almacenamiento externo debe garantizar distancia suficiente para proteger las copias de desastres que afecten la ubicación principal.
2. **Controles de seguridad:**
   * Los sitios de almacenamiento deben contar con certificaciones en gestión de seguridad de la información cuando sea posible

.

* + Las instalaciones deben tener medidas de protección física, lógica y ambiental, incluyendo control de temperatura, acceso restringido y monitoreo constante.

**Planificación y ejecución de respaldos:**

1. **Frecuencia y programación:**
   * Las copias de respaldo se realizarán de acuerdo con un plan aprobado por el Grupo TICS y el Oficial de Seguridad de la Información.
   * La frecuencia de los respaldos dependerá de la criticidad de los sistemas e información, pero debe garantizar la restauración completa en caso de incidente.
2. **Mecanismos de respaldo:**
   * Se emplearán tecnologías avanzadas que permitan copias incrementales, completas y diferenciales según las necesidades del sistema.
   * Las imágenes de sistemas operativos críticos serán respaldadas para garantizar una rápida recuperación en caso de fallos.

**Pruebas y restauración:**

1. **Pruebas periódicas:**
   * Los procedimientos de restauración se verificarán y probarán trimestralmente para garantizar su eficacia.
   * Los resultados de estas pruebas se documentarán y reportarán al Oficial de Seguridad de la Información y a la Oficina de Control Interno.
2. **Documentación y trazabilidad:**
   * Cada actividad de respaldo y restauración debe registrarse, incluyendo fecha, tipo de respaldo, ubicación de almacenamiento y responsables.
   * Los registros deben estar disponibles para auditorías internas y externas.

**Gestión de contingencias:**

1. **Plan de recuperación:**
   * Se establecerá un plan de recuperación que detalle los pasos a seguir en caso de contingencias que requieran la restauración de información.
   * Este plan incluirá responsables, tiempos estimados y prioridades según la criticidad de los sistemas afectados.
2. **Mecanismos de acceso:**
   * Solo el personal autorizado podrá acceder a los medios de respaldo y procedimientos de restauración.
   * Los medios de respaldo serán cifrados para proteger su contenido durante el almacenamiento y transporte.

**Concienciación y capacitación:**

* + Los usuarios serán capacitados regularmente sobre la importancia de los respaldos y su rol en la protección de la información.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, incluyendo usuarios, colaboradores y terceros que interactúen con los activos de información y sistemas del Ministerio de Minas y Energía.

**Nivel de cumplimiento de la política**

El cumplimiento es obligatorio y debe alcanzar el 100% por parte de todas las personas involucradas. El incumplimiento será gestionado conforme a los procedimientos disciplinarios establecidos.

**Excepciones**

Cualquier excepción debe ser autorizada formalmente por el Grupo TICS y el Oficial de Seguridad de la Información, y revisada por la Mesa de Continuidad y Gestión del Cambio o quien haga sus veces.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en las necesidades de respaldo, normativas o riesgos asociados, garantizando su relevancia y adecuación.

### 7.2.21 Política de registro de eventos

**Objetivo de la política**

Registrar eventos y generar evidencia que permita detectar conductas o usos no autorizados en entornos y activos de información clasificados como confidenciales. Esta política busca mitigar riesgos asociados a incidentes de seguridad mediante la recolección, almacenamiento y análisis de registros relevantes.

**Política general**

El Ministerio de Minas y Energía establece un sistema integral de registro y auditoría de eventos, diseñado para documentar actividades del usuario, excepciones, fallas y eventos de seguridad de la información. Este sistema, basado en estándares de buenas prácticas, permite generar evidencia confiable para la detección temprana de amenazas, así como para la toma de decisiones informadas ante incidentes.

**Recolección de registros:**

Los registros de auditoría incluirán información clave que permita rastrear actividades relevantes, tales como:

* Identificación del usuario.
* Fecha y hora de inicio y finalización de actividades.
* Ubicación o identificador de terminal cuando aplique.
* Intentos exitosos y fallidos de acceso a sistemas y datos.
* Acciones realizadas sobre activos de información clasificados.

Estos registros se generarán automáticamente y serán almacenados en un equipo o sistema distinto al que los produce, garantizando su integridad y disponibilidad.

**Protección de los registros:**

Para evitar la manipulación o pérdida de información, se implementarán medidas de seguridad como:

* Controles que protejan los registros contra cambios no autorizados, incluyendo la edición o eliminación de archivos log.
* Monitoreo de la capacidad de almacenamiento para prevenir fallos o sobreescrituras.
* Sistemas de respaldo para los registros, asegurando su conservación en entornos seguros.

**Gestión y retención:**

1. **Definición de plazos:**
   * Los registros se conservarán durante los períodos establecidos por requisitos legales, contractuales o normativos aplicables.
   * El cronograma de depuración será definido por los Propietarios de la Información, en conjunto con la Oficina de Control Interno y el Oficial de Seguridad de la Información.
2. **Revisión periódica:**
   * Las actividades del administrador y operador del sistema se revisarán regularmente para identificar anomalías.
   * Los registros serán objeto de auditorías periódicas para garantizar su relevancia y utilidad.

**Detección y respuesta:**

El análisis continuo de los registros permitirá:

* Detectar patrones anómalos que puedan indicar actividades no autorizadas.
* Generar alertas tempranas para mitigar riesgos antes de que escalen.
* Proveer evidencia en caso de investigaciones relacionadas con incidentes de seguridad.

**Concienciación y capacitación:**

Se capacitará a los usuarios y administradores sobre la importancia del registro de eventos y su rol en la protección de la seguridad de la información. Esto incluye:

* Buenas prácticas en el manejo de sistemas.
* Responsabilidades individuales en la generación y protección de registros.
* Procedimientos para reportar incidentes detectados a través de análisis de logs.

**Alcance/Aplicabilidad**

Esta política aplica a todos los usuarios, colaboradores y encargados de plataformas IT y seguridad informática del Ministerio de Minas y Energía, así como a terceros que interactúen con sus sistemas.

**Nivel de cumplimiento de la política**

El cumplimiento es obligatorio para todas las partes involucradas. Cualquier incumplimiento será tratado conforme a los procedimientos disciplinarios establecidos por el Ministerio.

**Excepciones**

Cualquier excepción debe ser aprobada formalmente por el Oficial de Seguridad de la Información y revisada por la Mesa de Continuidad y Gestión del Cambio.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los sistemas, normativas o riesgos asociados, asegurando su relevancia y adecuación a las necesidades del Ministerio.

**7.2.22 Política de gestión de la vulnerabilidad técnica**

**Objetivo de la política**

Garantizar la obtención de información oportuna sobre las vulnerabilidades técnicas en los sistemas, aplicativos o activos de información de la Entidad, evaluar el nivel de compromiso de los activos respecto a estas vulnerabilidades y tomar las acciones correctivas necesarias para mitigar los riesgos asociados.

**Política general**

El Ministerio de Minas y Energía implementa un proceso integral para la gestión de vulnerabilidades técnicas, alineado con los procedimientos de control de cambios y respuesta a incidentes. Este proceso asegura la identificación, evaluación, priorización y mitigación de las vulnerabilidades que puedan comprometer la seguridad de la información y los sistemas críticos de la Entidad.

**Gestión de vulnerabilidades:**

1. **Roles y responsabilidades:**
   * Se asignan roles específicos para la gestión de vulnerabilidades, que incluyen el seguimiento de las mismas, valoración de riesgos asociados, implementación de parches y monitoreo continuo de los activos de información.
   * El Oficial de Seguridad de la Información supervisará el cumplimiento de estas responsabilidades, coordinando con el Grupo TICS y los propietarios de los activos.
2. **Identificación de vulnerabilidades:**
   * Se utilizarán recursos confiables como listas de entidades reconocidas que publican vulnerabilidades, herramientas automatizadas de análisis de seguridad y canales de reporte interno.
   * Los análisis de vulnerabilidades programados generarán entradas clave para la priorización de las acciones correctivas.
3. **Tiempos de respuesta:**
   * Se definirán tiempos de respuesta específicos según la criticidad del activo y el nivel de riesgo asociado a la vulnerabilidad detectada.
   * Las vulnerabilidades críticas deben ser atendidas de manera prioritaria para minimizar el impacto.
4. **Evaluación de riesgos:**
   * Cada vulnerabilidad identificada será sometida a una evaluación de riesgos que considere el tipo de activo afectado, su impacto potencial y las posibles medidas de mitigación.
   * Las vulnerabilidades que representen mayor riesgo para la confidencialidad, integridad o disponibilidad de la información serán priorizadas.
5. **Registro y auditoría:**
   * Se generarán registros detallados de todas las actividades relacionadas con la gestión de vulnerabilidades, incluyendo detección, evaluación, aplicación de parches y validación de soluciones implementadas.
   * Estos registros serán auditados periódicamente para garantizar la efectividad y cumplimiento del proceso.
6. **Revisión y mejora continua:**
   * El proceso de gestión de vulnerabilidades será revisado regularmente para evaluar su efectividad y realizar ajustes que respondan a nuevos desafíos tecnológicos o amenazas emergentes.
   * Las lecciones aprendidas de incidentes previos se integrarán en los procedimientos para mejorar las capacidades de prevención y respuesta.

**Integración con otros procesos:**

La gestión de vulnerabilidades se alinea con los siguientes procedimientos clave:

* **Control de cambios:** Asegurando que la implementación de parches o modificaciones necesarias no afecten negativamente la operatividad o seguridad de los sistemas.
* **Respuesta a incidentes:** Facilitando una coordinación ágil entre los equipos responsables para abordar vulnerabilidades que deriven en incidentes de seguridad.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, incluyendo usuarios, colaboradores y terceros que interactúen con los sistemas y activos de información del Ministerio de Minas y Energía.

**Nivel de cumplimiento de la política**

El cumplimiento de esta política es obligatorio para todas las personas involucradas. El incumplimiento será tratado como una violación de las políticas de seguridad y gestionado conforme a los procedimientos disciplinarios establecidos por el Ministerio.

**Excepciones**

Cualquier excepción debe ser formalmente justificada, aprobada por el Oficial de Seguridad de la Información y revisada por la Mesa de Continuidad y Gestión del Cambio.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en las normativas, tecnologías o riesgos asociados, garantizando su adecuación y efectividad en el contexto operativo del Ministerio.

### 7.2.23 Política de restricciones sobre la instalación de software

**Objetivo de la política**

Controlar la instalación de software en los sistemas operativos de los equipos del Ministerio de Minas y Energía, asegurando que cualquier programa o aplicativo instalado cumpla con los estándares de seguridad y esté alineado con las necesidades institucionales.

**Política general**

El Ministerio de Minas y Energía implementa medidas restrictivas sobre la instalación de software en sus equipos para prevenir riesgos asociados a programas no autorizados, garantizar la estabilidad de los sistemas y proteger la información institucional. Estas medidas incluyen un procedimiento formal para la solicitud, autorización e instalación de software.

**Restricciones y autorizaciones:**

1. **Prohibición de instalaciones no autorizadas:**
   * Ningún funcionario del Ministerio puede instalar software, programas o aplicaciones en los equipos institucionales sin la autorización formal correspondiente.
   * Esta restricción aplica tanto para los equipos utilizados en las oficinas como en la modalidad de teletrabajo.
2. **Procedimiento de autorización:**
   * En caso de necesitar la instalación de un nuevo software, el funcionario debe presentar una solicitud escrita y justificada a su jefe inmediato.
   * El jefe inmediato evaluará la solicitud y, si la considera pertinente, escalará el requerimiento al Grupo TICS de la Entidad.
   * El Grupo TICS es la única área autorizada para realizar la instalación de software en los equipos institucionales.

**Criterios para la evaluación del software:**

1. **Compatibilidad y seguridad:**
   * El software solicitado debe ser compatible con los sistemas operativos y plataformas utilizadas por el Ministerio.
   * Se verificará que el software no represente riesgos de seguridad, como vulnerabilidades conocidas o inclusión de códigos maliciosos.
2. **Licenciamiento:**
   * Solo se permite la instalación de software con licencias válidas y debidamente adquiridas, cumpliendo con las normativas de propiedad intelectual.
   * El Grupo TICS gestionará la adquisición y renovación de licencias cuando sea necesario.
3. **Necesidad institucional:**
   * El software solicitado debe responder a necesidades específicas de las funciones laborales y estar alineado con los objetivos de la Entidad.

**Monitoreo y cumplimiento:**

El Grupo TICS implementará herramientas y procedimientos para monitorear los equipos y detectar posibles instalaciones no autorizadas. Cualquier incumplimiento será gestionado conforme a los procedimientos disciplinarios establecidos por el Ministerio.

**Capacitación y concienciación:**

Se capacitará regularmente a los funcionarios sobre las políticas de instalación de software, enfatizando:

* Los riesgos asociados a la instalación de programas no autorizados.
* Los beneficios de cumplir con los procedimientos establecidos.
* Las responsabilidades individuales en el uso adecuado de los recursos tecnológicos.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, los usuarios, colaboradores del Ministerio de Minas y Energía, y cualquier tercero que utilice los activos de información del Ministerio.

**Nivel de cumplimiento de la política**

El cumplimiento de esta política es obligatorio para todas las personas involucradas. Cualquier incumplimiento será tratado como una violación de las normativas de seguridad y gestionado conforme a los procedimientos disciplinarios.

**Excepciones**

Cualquier excepción debe ser formalmente justificada, aprobada por el Grupo TICS y el Oficial de Seguridad de la Información, y revisada por la Mesa de Continuidad y Gestión del Cambio.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los sistemas, normativas o riesgos asociados, garantizando su relevancia y adecuación a las necesidades del Ministerio.

### 7.2.24 Política sobre auditorías de sistemas de información

**Objetivo de la política**

Obtener evidencias sobre los sistemas de información respecto al cumplimiento de los requisitos de seguridad y utilizar estas evidencias para implementar un proceso de mejora continua en la seguridad de la información.

**Política general**

El Ministerio de Minas y Energía realiza auditorías periódicas para evaluar y analizar la seguridad de los sistemas de información. Estas auditorías, llevadas a cabo por personal externo especializado, tienen como objetivo mejorar la seguridad, eficacia y eficiencia de los procesos, sistemas y componentes críticos.

**Lineamientos para las auditorías:**

1. **Frecuencia de auditorías:**
   * Las auditorías se realizarán al menos una vez al año o cuando haya cambios significativos en los impulsores clave del MSPI.
2. **Elementos auditados:**
   * Se evaluarán carpetas o repositorios, bases de datos, sitios web, equipos, software y servicios, verificando aspectos como sistemas antimalware, gestión de accesos y usuarios, cumplimiento legal, prevención de fraude, fuga de datos, actualizaciones de sistema y monitoreo de recursos.
3. **Tipos de auditorías:**
   * Se seleccionará el tipo de auditoría más adecuado según las necesidades identificadas, incluyendo:
     + Test de penetración.
     + Auditoría de red.
     + Auditoría de seguridad perimetral.
     + Auditoría web.
     + Auditoría forense.
     + Auditoría de cumplimiento legal.

**Monitoreo y mejora continua:**

Los resultados de las auditorías se documentarán y analizarán para identificar áreas de mejora. Estas acciones correctivas y preventivas se integrarán en los procesos de gestión de riesgos y seguridad de la información.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, los usuarios, colaboradores y terceros que interactúen con los sistemas de información y activos tecnológicos del Ministerio de Minas y Energía.

**Nivel de cumplimiento de la política**

El cumplimiento de esta política es obligatorio. Cualquier incumplimiento será tratado como una violación de las normativas internas y gestionado conforme a los procedimientos establecidos.

**Excepciones**

Cualquier excepción debe ser aprobada por el Oficial de Seguridad de la Información y revisada por la Mesa de Continuidad y Gestión del Cambio.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los sistemas, normativas o riesgos asociados, asegurando su vigencia y efectividad en el contexto operativo del Ministerio.

### 7.2.25 Política de gestión de la seguridad de las redes

**Objetivo de la política**

Asegurar la protección de la información que transita por las redes del Ministerio de Minas y Energía, garantizando la integridad, confidencialidad y disponibilidad de los datos mediante el establecimiento de controles y medidas de seguridad robustas para la gestión de sus redes y las instalaciones de procesamiento de información.

**Política general**

El Ministerio de Minas y Energía regula estrictamente las condiciones y requisitos para el tráfico en sus redes. Por medio del Grupo TICS y el Oficial de Seguridad de la Información, se supervisa que todas las conexiones y transferencias de datos cumplan con las políticas de seguridad establecidas y los controles necesarios para mitigar riesgos.

**Controles y medidas de seguridad en las redes:**

1. **Restricción del tráfico de red:**
   * El tráfico entre Internet y la red privada estará restringido mediante el uso de firewalls de perímetro configurados bajo el principio de "negar todo" por defecto.
   * Las configuraciones de fábrica de los firewalls serán reemplazadas por configuraciones seguras adaptadas a las necesidades específicas del Ministerio.
2. **Aprobación y documentación:**
   * Todos los cambios en las configuraciones de firewalls y routers deberán ser aprobados formalmente a través de un proceso documentado.
   * Los diagramas de arquitectura de red, incluyendo flujos de datos confidenciales, se mantendrán actualizados y disponibles para auditorías.
3. **Responsabilidades claras:**
   * Las reglas y configuraciones aplicadas a los elementos de red estarán bajo la supervisión exclusiva del personal autorizado del área de infraestructura, siguiendo los principios de separación de deberes y mínimo conocimiento.
   * Se documentarán y justificarán todas las reglas de firewall, manteniendo registros detallados de su creación y actualización.
4. **Monitoreo y auditorías:**
   * Todas las conexiones entrantes y salientes serán autorizadas, monitoreadas y registradas, asegurando que los accesos no autorizados sean identificados y gestionados.
   * Se generarán logs de acceso, modificaciones y eventos relacionados con los elementos de red, los cuales serán auditados periódicamente.
5. **Protección contra suplantación:**
   * Se implementarán mecanismos de detección y bloqueo de direcciones IP manipuladas para prevenir accesos fraudulentos.
   * Herramientas como Traducción de Dirección de Red (NAT) y servidores proxy se utilizarán para ocultar direcciones IP internas y reforzar la seguridad.
6. **Seguridad en equipos móviles:**
   * Todos los equipos móviles asignados deberán contar con firewalls de host configurados por el área de infraestructura, evitando manipulaciones no autorizadas.
7. **Servicios de red:**
   * Los mecanismos de seguridad, niveles de servicio y requisitos de gestión de los servicios de red estarán incluidos en acuerdos formales, ya sea para servicios internos o contratados externamente.
   * Estos acuerdos serán revisados y auditados periódicamente para garantizar su cumplimiento.
8. **Control de programas y servicios:**
   * Solo se instalarán y habilitarán programas, aplicativos y servicios necesarios para las funciones laborales autorizadas.
   * El acceso lógico a estos servicios será controlado tanto para usuarios como para administradores, configurando medidas de seguridad para evitar vulnerabilidades.
9. **Actualizaciones y mantenimiento:**
   * Las actualizaciones de seguridad se instalarán y verificarán periódicamente en todos los sistemas de red.
   * Procedimientos de mantenimiento proactivo garantizarán la disponibilidad y resiliencia de las redes.
10. **Monitoreo continuo:**
    * Las redes serán monitoreadas constantemente para prevenir accesos no autorizados y detectar actividades sospechosas.
    * Procedimientos documentados para la gestión de redes garantizarán una respuesta oportuna ante cualquier incidencia.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, incluyendo a los usuarios, colaboradores y terceros que utilicen las redes y activos de información del Ministerio de Minas y Energía.

**Nivel de cumplimiento de la política**

El cumplimiento de esta política es obligatorio para todas las partes involucradas. Cualquier incumplimiento será tratado conforme a los procedimientos disciplinarios establecidos por el Ministerio.

**Excepciones**

Cualquier excepción debe ser formalmente justificada, aprobada por el Grupo TICS y el Oficial de Seguridad de la Información, y revisada por la Mesa de Continuidad y Gestión del Cambio.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los sistemas, normativas o riesgos asociados, asegurando su vigencia y efectividad en el contexto operativo del Ministerio.

### 7.2.26 Política de transferencia de información y cifrado

**Objetivo de la política**

Garantizar la seguridad de la información transferida dentro del Ministerio de Minas y Energía y con cualquier entidad externa, asegurando su confidencialidad, integridad, disponibilidad y privacidad mediante controles y procedimientos efectivos.

**Política general**

El Ministerio de Minas y Energía establece procedimientos claros y controles mínimos para proteger la información durante su transferencia, ya sea interna o externa, asegurando que cumpla con los más altos estándares de seguridad. La información pública clasificada y reservada será tratada con especial atención, utilizando métodos seguros para su intercambio y evitando cualquier divulgación no autorizada.

**Controles y procedimientos para la transferencia de información:**

1. **Modelos de acuerdos de confidencialidad e intercambio de información:**
   * Se establecerán acuerdos de confidencialidad con proveedores y terceros, los cuales incluirán compromisos específicos y penalidades en caso de incumplimiento.
   * Los acuerdos deberán cubrir responsabilidades, procedimientos para la transmisión y recepción de información, trazabilidad, no repudio, y medidas para la protección de la información.
2. **Protección de la información transferida:**
   * Toda transferencia de información, ya sea por medios físicos o digitales, deberá utilizar mecanismos de autenticación, autorización y registro.
   * La información física, como documentos impresos, deberá estar resguardada en cajones cerrados bajo llave y utilizar embalajes con sellos de seguridad al ser transportada.
3. **Restricciones en el intercambio de información confidencial:**
   * Está prohibido el uso de correos electrónicos personales (Outlook, Gmail, entre otros) para la transmisión de información relacionada con el Ministerio.
   * La información clasificada no podrá ser transmitida por medios telefónicos o correo electrónico sin las protecciones necesarias, como cifrado y controles de acceso.
4. **Uso de tecnologías de cifrado:**
   * Para la información en formato digital, se emplearán soluciones tecnológicas de cifrado que garanticen la confidencialidad e integridad durante su transmisión.
   * Las direcciones IP y servidores proxy deberán ser configurados para evitar la exposición de datos sensibles.
5. **Manejo de información en medios físicos:**
   * Los documentos y otros medios físicos no deben abandonarse en áreas públicas, impresoras o espacios de circulación alta.
   * Se requiere reserva absoluta en conversaciones que involucren información sensible, limitándolas a áreas seguras dentro de la Entidad.
6. **Seguridad en plataformas digitales:**
   * Los intercambios de información entre usuarios de la página web del Ministerio deben cumplir con medidas de seguridad como sesiones seguras, generación de registros de auditoría y validez jurídica de los mensajes de datos.

**Acuerdos sobre transferencia de información:**

1. **Procesamiento de información con proveedores:**
   * Cualquier convenio con proveedores o terceros deberá garantizar la confidencialidad, integridad y auditabilidad de la información procesada, conforme a los estándares de Seguridad de la Información del Ministerio.
2. **Gestión de usuarios y auditoría:**
   * Los registros de auditoría serán obligatorios para todas las transferencias de información sensibles, asegurando la trazabilidad y validez de las operaciones realizadas.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, incluyendo usuarios, colaboradores y terceros que interactúen con los activos de información del Ministerio de Minas y Energía.

**Nivel de cumplimiento de la política**

El cumplimiento de esta política es obligatorio para todas las partes involucradas. Cualquier incumplimiento será tratado conforme a los procedimientos disciplinarios establecidos por el Ministerio.

**Excepciones**

Cualquier excepción debe ser formalmente justificada, aprobada por el Grupo TICS y el Oficial de Seguridad de la Información, y revisada por la Mesa de Continuidad y Gestión del Cambio.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los sistemas, normativas o riesgos asociados, garantizando su vigencia y efectividad en el contexto operativo del Ministerio.

### 7.2.27 Política de uso de correo electrónico

**Objetivo de la política**

Garantizar la protección adecuada de la información transmitida mediante mensajería electrónica institucional, asegurando que sea utilizada exclusivamente para fines laborales y cumpla con las políticas de seguridad de la información establecidas.

**Política general**

El Ministerio de Minas y Energía regula el uso del correo electrónico institucional para garantizar la confidencialidad, integridad y uso responsable de este medio. Todo contenido transmitido a través del correo institucional se considera propiedad del Ministerio, y su manejo indebido puede dar lugar a sanciones disciplinarias.

**Controles y responsabilidades:**

1. **Uso exclusivo del correo institucional:**
   * Toda comunicación interna y externa deberá realizarse a través del correo institucional aprobado por el Ministerio.
   * Queda prohibido el uso de cuentas de correo personales para fines laborales.
2. **Responsabilidad del contenido:**
   * Los usuarios son responsables de revisar y validar la información antes de enviarla, asegurando que no perjudique la imagen de la Entidad.
   * El contenido de los correos debe estar alineado con los principios éticos y normativos del Ministerio.
3. **Firma en correos:**
   * Todos los correos enviados deben incluir la firma institucional correspondiente del remitente.
4. **Gestión de correos sospechosos:**
   * Los correos electrónicos sospechosos o no solicitados deben ser reportados inmediatamente al Grupo TICS sin abrirlos.
   * Se implementarán medidas para evitar que correos maliciosos afecten los sistemas del Ministerio.
5. **Monitoreo y auditoría:**
   * El Ministerio se reserva el derecho de monitorear el uso del correo institucional para garantizar su cumplimiento con las políticas establecidas.
   * Este monitoreo será llevado a cabo por el Oficial de Seguridad de la Información en coordinación con la Alta Dirección, sin acceso al contenido privado de los mensajes salvo autorización específica.
6. **Prohibición de compartir credenciales:**
   * Los usuarios no deben compartir las credenciales de acceso a sus cuentas de correo institucional con terceros bajo ninguna circunstancia.

**Uso de internet:**

1. **Propósitos laborales:**
   * El servicio de internet debe ser utilizado exclusivamente para actividades laborales. Su uso indebido será investigado y sancionado.
   * La navegación debe ser razonable y enfocada en propósitos laborales legítimos.
2. **Restricción de redes sociales:**
   * El uso de redes sociales está restringido, salvo para dependencias autorizadas que gestionen publicaciones institucionales con asesoramiento previo del Oficial de Seguridad de la Información.
3. **Prohibiciones específicas:**
   * Está prohibido acceder a sitios web que promuevan contenidos contrarios a la moral, buenas costumbres o la ley.
   * No se permite descargar programas ni almacenar información personal sin autorización institucional.

**Acuerdos de confidencialidad:**

1. **Identificación y documentación:**
   * Los requisitos de confidencialidad o no divulgación se identificarán, revisarán regularmente y documentarán conforme a las necesidades del Ministerio.
2. **Cláusulas en contratos y convenios:**
   * Todos los convenios o contratos con funcionarios, contratistas y personal externo incluirán cláusulas de confidencialidad y reserva de información.
   * Estas cláusulas serán monitoreadas para garantizar su cumplimiento.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, incluyendo a los usuarios, colaboradores y terceros que interactúen con los sistemas de correo electrónico e internet del Ministerio de Minas y Energía.

**Nivel de cumplimiento de la política**

El cumplimiento de esta política es obligatorio para todas las partes involucradas. Cualquier incumplimiento será tratado conforme a los procedimientos disciplinarios establecidos.

**Excepciones**

Cualquier excepción a esta política debe ser formalmente justificada, aprobada por el Grupo TICS y el Oficial de Seguridad de la Información, y revisada por la Mesa de Seguridad y Privacidad de la Información.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los sistemas, normativas o riesgos asociados, asegurando su vigencia y adecuación a las necesidades del Ministerio.

### 7.2.28 Política para adquisición, desarrollo y mantenimiento seguro de software

**Objetivo de la política**

Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo su ciclo de vida, incluyendo los requisitos para sistemas que prestan servicios sobre redes públicas, garantizando su confidencialidad, integridad y disponibilidad.

**Política general**

El Ministerio de Minas y Energía garantiza que la seguridad de la información esté integrada en cada etapa del ciclo de vida de los sistemas de información, desde su adquisición hasta su desarrollo y mantenimiento. Esto incluye medidas específicas para proteger los sistemas desplegados en entornos públicos o web, asegurando que cumplan con estándares internacionales de codificación segura y gestión de riesgos.

**Principios de adquisición y desarrollo seguro:**

1. **Construcción y adquisición:**
   * Todo software adquirido o desarrollado, ya sea internamente o a través de terceros, debe cumplir con principios de seguridad desde su codificación hasta su implementación.
   * Los desarrollos deberán seguir las directrices de OWASP (Open Web Application Security Project), que forman parte de la metodología de desarrollo seguro adoptada por el Grupo TICS.
2. **Gestión de riesgos:**
   * Los riesgos de seguridad de la información deben ser evaluados y gestionados durante todo el proceso de adquisición y desarrollo.
   * Cada desarrollo será sometido a análisis de vulnerabilidades y pruebas exhaustivas antes de su implementación.
3. **Revisión de código:**
   * Todo código fuente será revisado en busca de errores de codificación, fallos funcionales o vulnerabilidades antes de ser implementado en producción.
   * Los códigos modificados durante el ciclo de desarrollo o después de pruebas deberán pasar por una nueva revisión.
4. **Auditorías y pruebas:**
   * Se realizarán auditorías técnicas sobre el software para garantizar su funcionalidad, eficiencia y seguridad.
   * Todas las correcciones encontradas deberán ser implementadas antes de que el software pase a producción.

**Requisitos de seguridad:**

1. **Definición de requisitos:**
   * Los requisitos de seguridad serán parte integral de las especificaciones para nuevos sistemas y actualizaciones de sistemas existentes.
   * Se documentarán requisitos específicos relacionados con la confidencialidad, integridad y disponibilidad de la información procesada.
2. **Servicios en redes públicas:**
   * Las aplicaciones que operen en entornos web deben seguir ciclos de desarrollo que incluyan análisis de riesgos, gestión de vulnerabilidades y pruebas de seguridad específicas.
   * Los servicios estarán protegidos contra actividades fraudulentas, divulgación no autorizada y alteraciones no autorizadas de mensajes.

**Gestión de cambios y mantenimiento:**

1. **Revisión técnica de aplicaciones:**
   * Cada cambio en las plataformas operativas será evaluado para garantizar que no impacte negativamente en la funcionalidad o seguridad de las aplicaciones.
   * Las aplicaciones críticas serán sometidas a pruebas de compatibilidad y desempeño tras cada cambio.
2. **Restricciones a cambios:**
   * Los cambios a paquetes de software serán realizados exclusivamente por personal autorizado del Grupo TICS.
   * Si es necesario que un proveedor realice modificaciones, estas serán supervisadas por el Grupo TICS para proteger la confidencialidad y la integridad de la información.

**Pruebas de seguridad de sistemas:**

Se implementarán programas de pruebas exhaustivas para garantizar la calidad y seguridad del software:

1. **Compatibilidad:** Verificar el funcionamiento en diversas plataformas (hardware, sistemas operativos, redes, etc.).
2. **Integración:** Asegurar la conectividad entre módulos del software y otros sistemas relacionados.
3. **Funcionalidad:** Confirmar que el software cumple con los objetivos establecidos.
4. **Desempeño:** Evaluar la eficiencia del sistema bajo condiciones normales y de carga.
5. **Instalación:** Validar la correcta instalación en los servidores destinados.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, incluyendo usuarios, colaboradores, desarrolladores y terceros que interactúen con los sistemas y activos de información del Ministerio de Minas y Energía.

**Nivel de cumplimiento de la política**

El cumplimiento de esta política es obligatorio. Cualquier incumplimiento será tratado conforme a los procedimientos disciplinarios establecidos.

**Excepciones**

Cualquier excepción debe ser formalmente justificada, aprobada por el Grupo TICS y el Oficial de Seguridad de la Información, y revisada por la Mesa de Continuidad y Gestión del Cambio.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los sistemas, normativas o riesgos asociados. Las revisiones incluirán una evaluación exhaustiva de su pertinencia y eficacia en el contexto operativo del Ministerio, garantizando que los procedimientos reflejen las mejores prácticas y respondan a las necesidades emergentes de la Entidad.

### 7.2.29 Política de relaciones con proveedores

**Objetivo de la política**

Asegurar la protección de los activos de información de la Entidad que sean accesibles a los proveedores, mediante el establecimiento de controles y acuerdos claros que garanticen el cumplimiento de las políticas de seguridad de la información.

**Política general**

El Ministerio de Minas y Energía implementa mecanismos de control en las relaciones con los proveedores, asegurando que estos cumplan con las políticas, normas y procedimientos de seguridad de la información aplicables. Esto incluye acuerdos de confidencialidad, visitas de inspección y monitoreo continuo de sus actividades relacionadas con los activos del Ministerio.

**Controles y responsabilidades:**

1. **Divulgación y aceptación de políticas:**
   * Los responsables de gestionar contratos con proveedores deben garantizar la divulgación, entendimiento y aceptación de las políticas de seguridad del Ministerio.
   * Estas políticas serán anexadas como un punto adicional en los contratos, validados previamente por el Grupo de Gestión Contractual.
2. **Monitoreo de proveedores críticos:**
   * El Oficial de Seguridad de la Información, junto con las partes responsables, realizará visitas anuales a proveedores críticos para evaluar el cumplimiento de los requisitos de seguridad.
   * Estas visitas serán apoyadas por la Oficina de Control Interno cuando sea necesario.
3. **Acuerdos de confidencialidad:**
   * Antes de iniciar cualquier relación contractual, se firmará un acuerdo de confidencialidad que detalle el tipo de información intercambiada, medios utilizados, frecuencia y procedimientos de protección.
   * El cumplimiento de estos acuerdos será verificado periódicamente por el Oficial de Seguridad de la Información y la Oficina de Control Interno.
4. **Revisión de equipos y comunicaciones:**
   * Se evaluarán las condiciones de seguridad de los equipos tecnológicos de los proveedores críticos antes de permitir su conexión a la red del Ministerio.
   * Las configuraciones de comunicación segura, cifrado y transmisión de información serán revisadas regularmente.
5. **Monitoreo continuo:**
   * Los supervisores de contratos, junto con el Oficial de Seguridad de la Información, monitorearán el cumplimiento de acuerdos de nivel de servicio, confidencialidad y eliminación segura de información por parte de los proveedores.
   * Se realizará seguimiento a la gestión de riesgos y a los compromisos asumidos en materia de seguridad.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, los usuarios, colaboradores y proveedores que interactúen con los activos de información del Ministerio de Minas y Energía.

**Nivel de cumplimiento de la política**

El cumplimiento de esta política es obligatorio. Cualquier incumplimiento será tratado conforme a los procedimientos disciplinarios establecidos.

**Excepciones**

Cualquier excepción debe ser formalmente justificada, aprobada por el Oficial de Seguridad de la Información, y revisada por la Mesa de Seguridad y Privacidad de la Información.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los sistemas, normativas, contratos o riesgos asociados. Las revisiones incluirán evaluaciones detalladas para garantizar que las relaciones con los proveedores cumplan con los estándares de seguridad establecidos por el Ministerio.

**7.2.30 Política para gestión de incidentes**

**Objetivo de la política**

Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad, debilidades y la mitigación de sus impactos.

**Política general**

El Ministerio de Minas y Energía promueve la identificación, reporte y gestión eficaz de los incidentes de seguridad de la información que puedan comprometer la confidencialidad, integridad, disponibilidad o privacidad de los activos de información. La política abarca incidentes digitales y no digitales, y establece un marco de referencia para su tratamiento adecuado.

**Gestión de incidentes:**

1. **Roles y responsabilidades:**
   * El Oficial de Seguridad de la Información, apoyado por la Mesa de Trabajo de Seguridad y Privacidad, liderará la gestión de incidentes, incluyendo evaluación de impacto, toma de decisiones y coordinación de acciones de respuesta.
   * La Alta Dirección es responsable de reportar incidentes relevantes a las autoridades competentes previa validación de la Oficina Asesora Jurídica del Ministerio.
2. **Notificación y reporte:**
   * Cualquier parte interesada debe reportar incidentes potenciales o reales mediante canales establecidos, incluyendo comunicación telefónica, correo electrónico o verbal al Coordinador del Grupo TICS.
   * Los incidentes serán priorizados y tratados de acuerdo con su criticidad, siguiendo procedimientos aprobados por el Oficial de Seguridad de la Información.
3. **Registro y trazabilidad:**
   * Todos los incidentes serán registrados en un sistema centralizado, documentando detalles como fecha, hora, gravedad, recursos afectados, acciones realizadas y estado actual.
   * La Mesa de Ayuda del Grupo TICS garantizará la trazabilidad completa de los eventos reportados.

**Procedimientos específicos:**

1. **Detección y análisis:**
   * Se desplegarán herramientas de detección automática para identificar eventos sospechosos.
   * Los incidentes serán categorizados y evaluados en función de su impacto y prioridad.
2. **Respuesta y resolución:**
   * Se desarrollarán procedimientos para la recogida de evidencias, análisis forense, escalado y mitigación de daños.
   * Los incidentes más frecuentes y peligrosos tendrán respuestas predefinidas, con protocolos específicos para su tratamiento.
3. **Comunicación:**
   * Se definirá un punto de contacto único para la notificación de incidentes.
   * Los interesados recibirán orientación sobre acciones inmediatas a seguir.
4. **Cierre y aprendizaje:**
   * Una vez gestionado el incidente, se registrarán formalmente los resultados y las lecciones aprendidas.
   * Estas lecciones se utilizarán para ajustar procedimientos y fortalecer controles preventivos.

**Capacitación y sensibilización:**

* Los colaboradores recibirán capacitación periódica sobre registro y reporte de incidentes, entendiendo las implicaciones técnicas, disciplinarias y legales.
* La política fomentará una cultura de reporte proactivo, incentivando a los interesados a informar sobre debilidades o incidentes potenciales.

**Evaluación y mejora continua:**

* Se medirán indicadores de gestión de incidentes, analizando el impacto y la frecuencia para identificar áreas de mejora.
* Los procedimientos serán revisados anualmente o cuando un cambio significativo lo requiera, garantizando su eficacia.

**Recopilación de evidencias:**

1. **Cadena de custodia:**
   * Las evidencias recopiladas deben ser protegidas para mantener su integridad y utilidad legal.
   * Solo personal autorizado podrá manejar las evidencias.
2. **Repositorio centralizado:**
   * Se mantendrá un repositorio seguro con acceso restringido para almacenar información sobre incidentes y promover análisis futuros.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, sus usuarios, colaboradores y terceros que interactúen con los activos de información del Ministerio de Minas y Energía.

**Nivel de cumplimiento de la política**

El cumplimiento es obligatorio. Las infracciones serán gestionadas conforme a los procedimientos disciplinarios establecidos.

**Excepciones**

Cualquier excepción debe ser formalmente justificada, aprobada por el Oficial de Seguridad de la Información y revisada por la Mesa de Seguridad y Privacidad de la Información

**Revisiones**

Esta política será revisada anualmente o cuando se produzcan cambios significativos en los componentes del SGSI, del SGCN, del MSPI, en las partes interesadas o en la estructura interna del Ministerio. Cada revisión incluirá análisis detallados para garantizar que las prácticas de gestión de incidentes sean efectivas, estén alineadas con las mejores prácticas y respondan a las necesidades emergentes.

### 7.2.31 Políticas de cumplimiento

**Objetivo de la política**

Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con la seguridad de la información y cualquier otro requisito normativo aplicable, garantizando la adherencia a los estándares y leyes vigentes.

**Política general**

El Ministerio de Minas y Energía implementa un marco normativo integral que asegura el cumplimiento de los requisitos legales, estatutarios y contractuales. Esto incluye la identificación, documentación y actualización de las leyes aplicables al Sistema de Gestión de Seguridad de la Información (SGSI), así como la inclusión de los requisitos en contratos, acuerdos y proyectos.

**Requisitos legales y regulatorios:**

1. **Normativa aplicable:**
   * El Ministerio se adhiere a la norma ISO/IEC 27001:2022, que establece directrices para la gestión de la seguridad de la información, incluyendo roles, responsabilidades, identificación de activos, valoración de riesgos y auditorías del SGSI.
2. **Responsabilidades:**
   * La Alta Dirección, los dueños de procesos, el Oficial de Seguridad de la Información y otras áreas relacionadas deben garantizar el cumplimiento de los requisitos legales y regulatorios.
   * Se realizarán revisiones permanentes sobre la expedición de nuevas normativas y su impacto en la seguridad de la información.
3. **Manejo de incumplimientos:**
   * Cualquier posibilidad de incumplimiento será identificada, analizada y gestionada mediante acciones correctivas para mitigar los riesgos legales y contractuales.

**Derechos de propiedad intelectual:**

El Ministerio asegura el cumplimiento de las leyes relacionadas con los derechos de propiedad intelectual mediante:

* Políticas de licenciamiento que prohíben el uso de software no autorizado y la reproducción no autorizada de obras protegidas.
* Registros detallados de licencias, manuales y discos maestros.
* Auditorías periódicas para garantizar el uso adecuado del software.
* Implementación de controles sobre el número máximo permitido de usuarios y verificación de licencias instaladas.
* Divulgación de normativas relacionadas con la adquisición y uso de software.

**Protección de registros:**

1. **Clasificación y retención:**
   * Los registros críticos se protegerán contra pérdida, destrucción y falsificación.
   * Cada registro tendrá un periodo de retención definido y un medio de almacenamiento apropiado (papel, medios magnéticos u ópticos).
2. **Cumplimiento normativo:**
   * Algunos registros requerirán retención segura para cumplir con requisitos legales o respaldar actividades esenciales.

**Controles criptográficos:**

El Ministerio utiliza controles criptográficos en cumplimiento con legislación aplicable y acuerdos internacionales:

* Respetar las restricciones sobre importación y exportación de hardware y software criptográfico.
* Buscar asesoría legal antes de transferir información encriptada a través de fronteras jurisdiccionales.

**Revisión independiente:**

1. **Control Interno:**
   * Realizará revisiones independientes sobre la implementación de las políticas de seguridad de la información para garantizar su pertinencia y eficacia.
2. **Evaluación del SGSI:**
   * Se identificarán nuevos requerimientos normativos y se documentarán cambios necesarios al SGSI.

**Revisión de cumplimiento técnico:**

1. **Revisiones periódicas:**
   * Los sistemas serán revisados para evaluar su cumplimiento con las políticas y normas de seguridad.
2. **Pruebas de penetración:**
   * Estas pruebas se planificarán cuidadosamente para evitar comprometer la seguridad del sistema, asegurando su documentación y periodicidad.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, los usuarios, colaboradores y terceros que interactúen con los activos de información del Ministerio de Minas y Energía.

**Nivel de cumplimiento de la política**

El cumplimiento es obligatorio. Cualquier incumplimiento será tratado conforme a los procedimientos disciplinarios establecidos.

**Excepciones**

Cualquier excepción debe ser formalmente justificada, aprobada por el Oficial de Seguridad de la Información y revisada por la Mesa de Continuidad y Gestión del Cambio.

**Revisiones**

Esta política será revisada anualmente o cuando se produzcan cambios significativos en los sistemas, normativas, riesgos asociados o estructuras internas del Ministerio. Estas revisiones evaluarán la pertinencia, efectividad y alineación con las mejores prácticas, y se documentarán los ajustes requeridos para garantizar el cumplimiento normativo y la mejora continua.

### 7.2.32 Política de eliminación y destrucción segura de información

**Objetivo de la política**

Establecer lineamientos claros para manejar la información que ha cumplido su ciclo de vida, asegurando su eliminación permanente de manera segura para prevenir divulgaciones no autorizadas y proteger la confidencialidad de los activos de información del Ministerio de Minas y Energía.

**Política general**

El Ministerio de Minas y Energía define procedimientos específicos para la eliminación, destrucción y borrado seguro de información contenida en activos físicos y lógicos. Estas acciones forman parte integral de los controles de seguridad implementados para evitar la divulgación de información confidencial y sensible.

**Mecanismos de eliminación segura:**

1. **Eliminación de medios físicos:**
   * La información contenida en medios como USBs, discos duros y cintas de respaldo debe ser eliminada mediante técnicas seguras, incluyendo:
     + **Sobrescritura:** Escritura repetida de datos aleatorios sobre la información original.
     + **Desmagnetización:** Aplicación de campos magnéticos para borrar completamente los datos.
     + **Destrucción física:** Trituración o pulverización de los dispositivos para hacerlos irrecuperables.
2. **Eliminación de medios lógicos:**
   * El borrado seguro de información en sistemas lógicos debe realizarse según las mejores prácticas establecidas en las directrices del NIST. Esto incluye la utilización de herramientas especializadas para garantizar la irrecuperabilidad de los datos.
3. **Validación de cumplimiento:**
   * El Oficial de Seguridad de la Información y/o quien haga sus veces, con apoyo de la Oficina de Control Interno, verificará semestralmente que los procedimientos de eliminación segura se implementen correctamente, especialmente en equipos gestionados por proveedores.
4. **Gestión de cintas de respaldo:**
   * Las cintas de respaldo almacenadas en la Cintoteca del Archivo Central serán protegidas y gestionadas según estándares mínimos, garantizando su almacenamiento seguro hasta su eliminación.

**Responsabilidades:**

1. **Usuarios:**
   * Los usuarios y colaboradores deben garantizar que la información que ya no es necesaria sea gestionada según los procedimientos establecidos.
2. **Oficial de Seguridad de la Información:**
   * Supervisará la implementación y cumplimiento de los procedimientos de eliminación y destrucción segura.
   * Realizará capacitaciones sobre el manejo adecuado de la información al final de su ciclo de vida.
3. **Proveedores:**
   * Los proveedores responsables de la disposición final de activos físicos deben cumplir con los procedimientos de eliminación segura y presentar evidencias de cumplimiento.

**Alcance/Aplicabilidad**

Esta política aplica a toda la Entidad, incluyendo usuarios, colaboradores y terceros que interactúen con activos de información del Ministerio de Minas y Energía.

**Nivel de cumplimiento de la política**

El cumplimiento de esta política es obligatorio. Las violaciones serán gestionadas conforme a los procedimientos disciplinarios establecidos por el Ministerio.

**Excepciones**

Cualquier excepción a esta política debe ser formalmente justificada, aprobada por el Oficial de Seguridad de la Información y revisada por la Mesa de Continuidad y Gestión del Cambio.

**Revisiones**

Esta política será revisada anualmente o cuando ocurran cambios significativos en los sistemas, normativas, riesgos asociados o en la estructura interna del Ministerio. Estas revisiones evaluarán su pertinencia, efectividad y alineación con las mejores prácticas internacionales para garantizar la seguridad de la información eliminada.

# GLOSARIO

* **Activo de información:** Cualquier elemento de información que tenga valor para la Entidad, almacenado en cualquier medio. Este puede incluir bases de datos, documentos, correos electrónicos, código fuente, diseños y otros formatos. (Fuente: ISO/IEC 27001:2022).
* **Autorización:** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales. (Fuente: ISO/IEC 27002:2022).
* **Aviso de privacidad:** Comunicación generada por el responsable del tratamiento de datos personales para informar al titular sobre la existencia de políticas de tratamiento, las finalidades del tratamiento y cómo acceder a estas. (Fuente: Ley 1581 de 2012 y Manual de Tratamiento de Datos Personales de MINENERGÍA).
* **Base de datos:** Conjunto organizado de datos personales sometido a tratamiento. (Fuente: MINENERGÍA, Manual de Tratamiento de Datos Personales).
* **Categorías de información:** Agrupación de información homogénea basada en sus características internas (contenido) o externas (formato o estructura). Incluye información pública, clasificada, reservada y semiprivada. (Fuente: Ley 1712 de 2014 y Manual de Tratamiento de Datos Personales de MINENERGÍA).
* **Cifrado:** Proceso de convertir información legible en un formato codificado para evitar accesos no autorizados.
* **Confidencialidad:** Garantía de que la información está disponible solo para las personas autorizadas. (Fuente: ISO/IEC 27001:2022).
* **Control criptográfico:** Uso de herramientas criptográficas para garantizar la confidencialidad, integridad y autenticidad de la información durante su almacenamiento o transmisión. (Fuente: Ley 1266 de 2008 y Manual de Políticas de Seguridad de MINENERGÍA).
* **Dato personal:** Información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Fuente: Ley 1581 de 2012).
* **Dato público:** Datos no considerados privados o sensibles, como estado civil, profesión u oficio y calidad de servidor público. (Fuente: Ley 1581 de 2012).
* **Datos abiertos:** Datos primarios en formatos interoperables y de acceso libre, puestos a disposición por entidades públicas para fomentar la reutilización y creación de servicios derivados. (Fuente: Ley 1712 de 2014).
* **Datos sensibles:** Información que afecta la intimidad del titular o puede generar discriminación, como origen racial, salud, orientación sexual y datos biométricos. (Fuente: Ley 1581 de 2012).
* **Encargado del tratamiento:** Persona o entidad que realiza el tratamiento de datos personales por cuenta del responsable del tratamiento. (Fuente: Ley 1581 de 2012).
* **Gestor de incidentes:** Persona o equipo designado para gestionar y coordinar la respuesta a incidentes de seguridad, garantizando la mitigación de impactos.
* **Incidente de seguridad:** Evento adverso que afecta la confidencialidad, integridad o disponibilidad de la información. Incluye intentos de acceso no autorizado, malware y violaciones de políticas de seguridad.
* **Información:** Datos tratados en forma digital o no digital, utilizados como base para procesos misionales. Incluye bases de datos, correos electrónicos, documentos y otros formatos relevantes. (Fuente: ISO/IEC 27000).
* **Información clasificada:** Información que no debe ser divulgada por su naturaleza, ya que puede atentar contra la intimidad de su titular. Incluye información privada y semiprivada. (Fuente: Ley 1712 de 2014).
* **Información disponible:** Información solicitada o consultada por la ciudadanía que no está publicada en el sitio web de la Entidad. (Fuente: Ley 1712 de 2014).
* **Información privada:** Información relacionada con el ámbito privado de una persona, protegida por orden judicial o normativa específica. Ejemplos: historias clínicas y documentos privados. (Fuente: Sentencia T-729 de 2002).
* **Información pública:** Información generada por sujetos obligados en el desarrollo de sus funciones misionales. (Fuente: Ley 1712 de 2014).
* **Información pública clasificada:** Información no divulgable que afecta derechos de privacidad de personas naturales o jurídicas. (Fuente: Ley 1712 de 2014).
* **Información pública reservada:** Información exceptuada de acceso público por daño a bienes o intereses públicos, cumpliendo con requisitos del Art. 19 de la Ley 1712 de 2014.
* **Información publicada:** Documentación disponible en el sitio web oficial de la Entidad. (Fuente: Ley 1712 de 2014).
* **Información semiprivada:** Información que no tiene naturaleza íntima ni pública, como datos financieros o comerciales de una persona. (Fuente: Ley 1266 de 2008).
* **Integridad:** Propiedad de asegurar que la información no ha sido alterada de manera no autorizada. (Fuente: ISO/IEC 27001:2022).
* **Mesa de Trabajo de Seguridad:** Grupo conformado para evaluar, coordinar y tomar decisiones relacionadas con la seguridad de la información y la continuidad del negocio en la Entidad.
* **Norma ISO/IEC 27001:2022:** Estándar internacional para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), enfocado en la protección de activos y mitigación de riesgos relacionados con la información.
* **Norma NIST 800-88:** Directrices del Instituto Nacional de Estándares y Tecnología (NIST) para el borrado seguro de datos, incluyendo técnicas para la eliminación física y digital.
* **Protección de registros:** Procedimientos implementados para prevenir la pérdida, destrucción o alteración no autorizada de registros críticos.
* **Responsable del tratamiento:** Persona o entidad que decide sobre el tratamiento de los datos personales. (Fuente: Ley 1581 de 2012).
* **Transferencia:** Envió de datos personales a un receptor, dentro o fuera del país, responsable del tratamiento. (Fuente: Ley 1581 de 2012).
* **Transmisión:** Comunicación de datos personales para su tratamiento por un encargado por cuenta del responsable. (Fuente: Ley 1581 de 2012).
* **Tratamiento:** Operaciones realizadas sobre datos personales, como recolección, almacenamiento, uso y supresión. (Fuente: Ley 1581 de 2012).
* **Titular:** Persona natural cuyos datos personales sean objeto de tratamiento. (Fuente: MINENERGÍA, Manual de Tratamiento de Datos Personales).

# REFERENCIAS

* Gobierno de Colombia. (2017). Guía para clasificación de la información. Presidencia de la República de Colombia.
* International Organization for Standardization. (2022). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.
* International Organization for Standardization. (2022). ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. ISO.
* International Organization for Standardization. (2022). ISO/IEC 27000:2022. Information security, cybersecurity and privacy protection — Overview and vocabulary. ISO.
* MINTIC. (2016, junio 2). Lo que usted debe saber del Conpes de Seguridad Digital. Ministerio de Tecnologías de la Información y las Comunicaciones. Recuperado de <https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/15410:Lo-que-usted-debe-saber-del-Conpes-de-Seguridad-Digital>.
* National Institute of Standards and Technology. (2020, junio 21). CSRC NIST - Computer Security Resource Center. Recuperado de <https://csrc.nist.gov/glossary>.
* National Institute of Standards and Technology. (2020). NIST Special Publication 800-88 Rev.1: Guidelines for Media Sanitization. Recuperado de <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>.