



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MINENERGÍA

Contenido

INTRODUCCIÓN.....	3
1. CONTEXTUALIZACIÓN.....	4
2. ANTECEDENTES	5
3. DEFINICIONES	6
4. OBJETIVOS	11
4.1. OBJETIVO GENERAL	11
4.2. OBJETIVOS ESPECIFICOS	11
5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	12
5.1. ALCANCE	12
5.2. POLÍTICAS	12
5.2.1. Creación de políticas	12
5.2.2. Aprobación de políticas	12
5.2.3. Actualización de políticas	12
5.2.4. Nombre de las políticas	13
5.2.5. Estructura de la política	13
5.2.6. Reglas de escritura de las políticas	13
5.2.7. Nivel de cumplimiento de la política	13
5.3. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	13
5.3.1. Política general.....	13
5.4. PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN	14
5.5. ROLES Y RESPONSABILIDADES	14
5.5.1. La Oficina del Despacho del Ministro(a):.....	15
5.5.2. Oficial de Seguridad de la Información o quien haga sus veces	16
5.5.3. Mesas de trabajo de seguridad y privacidad de la información	17
5.5.4. Responsable de los riesgos de seguridad de la información.....	17
5.5.5. Responsabilidades de las partes interesadas	17
5.5.6. Responsabilidades de proveedores	18
5.5.7. Analista seguridad de la información.....	18
5.5.8. Grupo de Infraestructura Tecnológica:	19



5.6. GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN.....	19
5.6.1. Definición.....	20
5.6.2. Revisión.....	20
5.6.3. Actualización	20
5.6.4. Publicación	21
5.7. PROTECCIÓN DE DATOS PERSONALES.....	21
5.8. CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN	21
5.8.1. Clasificación de acuerdo con la confidencialidad.....	21
5.8.2. Clasificación de acuerdo con la integridad y disponibilidad	22
5.9. ETIQUETADO DE ACTIVOS DE INFORMACIÓN.....	23
5.10. GESTIÓN DOCUMENTAL DEL MSPI	23
5.10.1. Ventajas de la integración.....	23
Las ventajas de la integración son las siguientes:.....	23
5.10.2. Creación y actualización de documentación	24
5.10.3. Control de la información documentada.....	24
5.11. GESTIÓN DE RIESGOS	25
5.11.1. Incidentes de la seguridad de la información	25
5.11.2. Eventos	26
5.12. VISIÓN GENERAL PARA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN	27
5.12.1. Establecimiento del contexto.....	28
5.12.2. Contexto interno y externo	28
5.12.3. Valoración de los riesgos	28
5.12.4. Seguimiento y monitoreo del Sistema de Gestión de Seguridad y Privacidad de la Información y del MSPI:.....	32
5.12.5 Auditorías internas.....	32
5.12.5. Revisión por parte de la alta dirección.	32
5.13. MEJORA CONTINUA DEL SGSI.....	32
5.13.1. Aseguramiento del Protocolo IPv6	33
5.13.2. Gestión y Clasificación de Incidentes de Seguridad de la Información.	33
6. CONCLUSIONES Y RECOMENDACIONES	38



INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información, es un producto de los esfuerzos realizados por el Ministerio de Minas y Energía, primero, con un diagnóstico y planeación para el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), con cubrimiento en los Sistemas de Gestión de Seguridad de la Información (SGSI) y Continuidad del Negocio (SGCN), con alcance a la fase PLANEAR del ciclo PHVA.

El dinamismo, evolución y actualización en los modelos, guías y normas, han permitido al Ministerio de Minas y Energía, desarrollar una segunda fase para realizar la actualización del Modelo de Seguridad y Privacidad de la información (MSPI), con sus sistemas asociados (SGSI-SGCN), ya con un alcance a las fases del HACER y parte del VERIFICAR, dentro del Ciclo PHVA.

De ahí la importancia que, el Ministerio de Minas y Energía, considere establecer un marco, en el cual, se asegure que la preservación de la confidencialidad, integridad y disponibilidad de la información que maneja, como producto del desarrollo su actividad, es protegida de manera adecuada, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, e-mail, transmitida en conversaciones, entre otros.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

El presente documento contiene los lineamientos del Modelo de Seguridad y Privacidad de la MSPI versión 3.0.2 definido por MINTIC, el cual orienta a las entidades a la preservación de la confidencialidad, integridad, disponibilidad de la información y permite fijar los criterios para proteger la privacidad de la información, los datos, así como de los procesos y las personas vinculadas con dicha información.

Para la elaboración de este documento, se toma como referencia además de los lineamientos de MINTIC en el MSPI y sus correspondientes guías de apoyo, la norma ISO 27001:2013 y el anexo A.

Las políticas de seguridad de la información incluidas en este documento constituyen una parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) y el Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno Digital y se convierten en la base para la implementación de los controles, procedimientos definidos por las normas anteriormente mencionadas.

Es responsabilidad de todas las partes interesadas del Ministerio de Minas y Energía velar por que no se realicen actividades que contradigan la esencia de este documento con el fin de preservar la confidencialidad, integridad y disponibilidad de la información que aquí se maneja.

1. CONTEXTUALIZACIÓN

Con el ánimo de asegurar la integridad, disponibilidad, confidencialidad y privacidad de la información de sus procesos, el Ministerio de Minas y Energía, está en el proceso de transformación e implementación del Plan de Seguridad y Privacidad de la información (MSPI), así como el Sistema de Seguridad de la Información (SGSI), para dar cumplimiento a la exigencia del Gobierno Nacional de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) de la política de Gobierno Digital así como la implementación del Sistema de Gestión de Seguridad de la Información, propendiendo de igual forma por los derechos como el habeas data, la imagen, la intimidad, el buen nombre y la privacidad.



2. ANTECEDENTES

En el pasado el Ministerio de Minas y Energía, contrato la elaboración de un diagnóstico y planeación para el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) y el Sistema de Gestión de Seguridad de la Información (SGSI) dando cumplimiento a lo estipulado la estrategia de Gobierno en línea.

El dinamismo, la evolución y actualización en los modelos, guías y norman le han permitido al Ministerio de Minias y Energía, desarrollar una segunda fase que le permitirá realizar la actualización e implementación del Sistema de Seguridad de la Información (SGSI), que integra el Modelo de Seguridad y Privacidad de la información (MSPI).

3. DEFINICIONES

Aceptación de riesgo: Decisión de asumir un riesgo.

Activo: Cualquier cosa que tiene valor para la organización.

Adaptabilidad: Define los eventos y bajo qué criterios un sistema debe poder ser monitoreado y revisado para su control posterior.

Amenazas: ¹Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.

Análisis de Riesgo: ²Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo aceptable.

Auditoria: ³Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidad.

Capacity Planning: Es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

Centros de cableado: Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Criptografía: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

¹ ISO/IEC 27000

² ISO/IEC 27000

³ ISO/IEC 27000



Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información. **Confidencialidad:** es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Ciberseguridad⁴: Capacidad del Estado para minimizar el nivel de riesgo aceptable al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Comité de Seguridad de la Información: El Comité de Seguridad de la Información, es un cuerpo integrado por representantes designados por la Alta Dirección con el objetivo de garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

Confiabilidad de la Información: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo aceptado. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. **Declaración de aplicabilidad:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo particular

Custodio del activo de información: Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados. **Derechos de Autor:** es un conjunto.

Dato personal: Es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

⁴ CONPES 3701

Declaración de aplicabilidad: ⁵Listado que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la entidad, tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Declaración de aplicabilidad: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el mismo.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión de incidentes de seguridad de la Información: ⁶Proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Guía DAFP: Guía para la administración y gestión del riesgo del Departamento Administrativo de la Función Pública.

MSPI: Modelo de Seguridad y Privacidad de la información, comprende las acciones transversales a los demás procesos, tendientes a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.

⁵ ISO/IEC 27000

⁶ ISO/IEC 27000

Plan de continuidad del negocio: ⁷Plan orientado a permitir la continuación de las principales funciones misionales o críticas del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos: ⁸Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Partes interesadas: Persona u organización que puede afectar, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. Para la entidad son los funcionarios, servidores públicos, contratistas, proveedores, ciudadanos y agencias relacionadas con el MINENERGIA.

Política: Es el marco referencial o lineamiento general emitido por la Alta Dirección, que orienta para las actuaciones, conductas o funciones de los colaboradores y dependencias.

Procedimiento: Es la forma especificada para llevar a cabo una actividad o un proceso.

Proceso: Es un conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman entradas en resultados.

Protección a la duplicación: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grave una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

Recursos informáticos: Todos aquellos componentes de hardware y programas (software) que son necesarios para el buen funcionamiento y la optimización del trabajo con computadores y periféricos, tanto a nivel Individual, como colectivo u organizativo, sin dejar de lado el buen funcionamiento de estos.

Riesgo: Toda posibilidad de ocurrencia de aquella situación que pueda entorpecer el desarrollo normal de las funciones de la Entidad y le impidan el logro de sus objetivos.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: Nivel restante de riesgo después del tratamiento del riesgo.

Seguridad de la Información: ⁹Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.

⁷ ISO/IEC 27000

⁸ ISO/IEC 27000

⁹ NTC-ISO/IEC 17799:2006



Seguridad de la Información¹⁰: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información SGSI¹¹: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

SIGME: Sistema Integrado de Gestión del Ministerio de Minas y Energía.

Tecnología de la Información: Se refiere al hardware y software operado por la organización por un tercero que procese información en su nombre, para llevar a cabo una función propia del Ministerio de Minas y Energía

Trazabilidad¹²: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Tratamiento del riesgo: Proceso de selección e implementación de acciones de mejorar que permita gestionar el riesgo.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

Vulnerabilidad Debilidad de un activo o control que puede ser explotada por una o más amenazas.¹³

10 ISO/IEC 27000

11 ISO/IEC 27000

12 ISO/IEC 27000

¹³ ISO/IEC 27000



4. OBJETIVOS

4.1. OBJETIVO GENERAL

Cumplir con los requisitos de seguridad, definidos en un SGSI y el MSPI, de GEL, que ayudarán, mediante su implementación, a preservar la confidencialidad, integridad y disponibilidad de la información, así como la relación de los procedimientos asociados a las políticas establecidas que permitan asegurar la protección de esta.

4.2. OBJETIVOS ESPECIFICOS

4.2.1. Contribuir al incremento de la transparencia, frente a la gestión pública.

4.2.2. Dar lineamiento para la implementación de la gestión de la seguridad y privacidad de la información.

4.2.3. Alinear el marco de referencia de arquitectura empresarial con los principios de seguridad y privacidad de la información.



5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.1. ALCANCE

Los lineamientos del Modelo de seguridad y privacidad de la información (MSPI) y sus correspondientes guías de apoyo, serán aplicadas a los procesos estratégicos, misionales, de apoyo, de evaluación y control y especiales del Ministerio de Minas y Energía, por tal motivo, deberán ser conocidas y cumplidas por todas las partes interesadas, que accedan a los sistemas de información, repositorios e instalaciones físicas.

5.2. POLÍTICAS

En el Ministerio de Minas y Energía se establece una política general la cual es generada desde el Sistema de Gestión de Seguridad de la Información SGSI y varias políticas generales en cumplimiento con el MSPI, teniendo en cuenta los siguientes criterios:

5.2.1. Creación de políticas

En el Ministerio de Minas y Energía deben ser creadas por el área encargada de la seguridad y privacidad de la información y respaldadas por la Alta Dirección de la entidad con la asesoría de las áreas técnicas responsables de los temas asociados a las mismas.

5.2.2. Aprobación de políticas

En el Ministerio de Minas y Energía, las políticas relacionadas con la seguridad y privacidad de la información deben ser aprobadas por la Alta Dirección con base en las recomendaciones del área encargada de la seguridad y privacidad de la información.

5.2.3. Actualización de políticas

Las políticas de seguridad y privacidad de la información se deben revisar periódicamente o si ocurren cambios significativos. Cualquier requerimiento de modificación, cambio o actualización de las políticas de seguridad y privacidad de la información, debe ser dirigida a la Alta Dirección con base en las recomendaciones del área encargada.

5.2.4. Nombre de las políticas

Siempre se hará referencia a las políticas de seguridad y privacidad de la información, y a la referencia del Anexo de la NTC ISO/IEC 27001:2013 y del MPSI al que hace referencia cada una.

5.2.5. Estructura de la política

La estructura de la Política de Seguridad es:

- Número de la política.
- Título de la política.
- Norma referente.
- Definición de la política.
- Objetivo.
- Alcance/Aplicabilidad.
- Nivel de cumplimiento.
- Responsable de la aprobación de política.
- Responsable de la política.
- Fecha de vigencia, de actualización y de retiro.

5.2.6. Reglas de escritura de las políticas

- Las políticas estarán escritas en forma sencilla y específica.
- El enunciado bien redactado y estará definido en un lenguaje técnico y explícito para los usuarios.

5.2.7. Nivel de cumplimiento de la política

Todas las personas cubiertas por el alcance y aplicabilidad deben dar cumplimiento del 100% de la política.

El incumplimiento a esta política traerá consigo, las consecuencias legales que apliquen a la normativa establecida por el Ministerio para tal fin, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

5.3. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.3.1. Política general



El Ministerio de Minas y Energía, está comprometido en proteger los activos de información de la Entidad (las partes interesadas internas y externas, la información como tal, los procesos, las tecnologías de información y comunicación incluido el hardware y el software que en su conjunto, soportan sus procesos), orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad y a la continuidad de las operaciones gestionando los riesgos de seguridad de la información y fomentando la creación de una cultura y conciencia de seguridad en los funcionarios fundamentados en la norma técnica colombiana NTC-ISO-27001:2013 y el modelo de seguridad y privacidad de la información (MSPI).

Lo expuesto hasta aquí, se encuentra sustentado en la resolución número 4-0362 del 03 de mayo de 2017.

5.4. PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Para el Ministerio de Minas y Energía, los procedimientos lineamientos e instructivos, constituyen una base importante para la preservación de la seguridad y privacidad de la información. Se han diseñado procedimientos, lineamientos e instructivos, que cubren las políticas de seguridad y privacidad de la información para los cuales han tenido en cuenta los 14 capítulos del Anexo A, definidas en la norma ISO/IEC 27001:2013 y los lineamientos de MINTIC a través del Modelo de Seguridad y Privacidad de la Información.

5.5. ROLES Y RESPONSABILIDADES

El Ministerio de Minas y Energía, con el ánimo de lograr el buen funcionamiento del Sistema de Gestión y Privacidad de la Información y el MSPI, particularizara los roles y responsabilidades de las personas que se van a encargar de establecer y desarrollar cada una de estas actividades asociadas a los sistemas.

Para la asignación de los responsables, el Ministerio analizará las funciones de cada rol comparándolas con el personal de la entidad, es necesario que las responsabilidades asignadas en el desarrollo del Sistema de Gestión de Seguridad y Privacidad de la Información y el MSPI, para cada perfil, sean incorporadas a los manuales de funciones de acuerdo con el cargo que desempeñan.

A continuación, se definen algunos roles y responsabilidades que se deben tener en cuenta en la implantación y seguimiento del Sistema de Gestión de Seguridad y Privacidad de la Información y el MSPI.

Recurso Humano	Rol	Responsabilidades
Ministro del MME	Alta Dirección	Apoyo implementación MSPI Gestión Estratégica
Mesa de Trabajo de Seguridad de la Información	Toma de decisiones	Toma de decisiones frente a la seguridad de la Información
Oficial de Seguridad de la Información o quien haga sus veces	Responsable MSPI	Liderazgo y responsabilidad del MSPI Gestión estratégica y táctica
Dueño del Riesgo	Gestión de Riesgos de seguridad de la Información	Gestión riesgos de seguridad de la información del proceso
Partes Interesadas	Cumplimiento MSPI	Dar estricto cumplimiento a lo estipulado en el MSPI.
Proveedores	Cumplimiento MSPI	Dar estricto cumplimiento a lo estipulado en el MSPI.
Analista Seguridad de la Información	Apoyo operativo de las actividades requeridas del MSPI	Gestión operativa y apoyo al Oficial de Seguridad de la Información o quien haga sus veces.
Grupo de Infraestructura Tecnológica.	Gestión de la transición y migración IPv4 a IPv6 Ejecución de actividades del MSPI	Llevar a cabo la implementación del protocolo IPv6 en la entidad. Orquestación de las partes interesadas. Cumplimiento del aseguramiento de IPv6 Gestión de riesgos tecnológicos de IPv6.

Tabla 1: Roles y Responsabilidades

5.5.1. La Oficina del Despacho del Ministro(a):

Como muestra de su compromiso en la dirección, gestión y apoyo en la implementación del MSPI, aprueba lo siguiente:

- Aprobar los objetivos de seguridad de la información, los cuales estarán alineados con los objetivos estratégicos de la entidad.
- Aprobar anualmente o cuando se requiera la Política de Seguridad y Privacidad de la Información del Ministerio y el plan MSPI.
- Asignar y aprobar el presupuesto necesario para el normal funcionamiento del SGSI, SGCN y MSPI.



- Garantizar que los requisitos del SGSI, SGCN y MSPI, se encuentran integrados en todos los procesos críticos de la entidad.
- Proporcionar los recursos necesarios para la implementación y desarrollo de las actividades del SGSI, SGCN y MSPI del Ministerio.
- Velar por la ejecución y desarrollo de las actividades del SGSI, SGCN y MSPI.
- Promover activamente una cultura de seguridad y privacidad de la información basada en riesgos para la entidad.
- Aprobar los roles y responsabilidades relacionados con la seguridad de la información en todos los niveles de la entidad y nombrar un “asesor” con rol de Oficial de Seguridad de la Información o quien haga sus veces y sus respectivos analistas para apoyo operativo.

5.5.2. Oficial de Seguridad de la Información o quien haga sus veces

Se recomienda al Ministerio de Minas y Energía, acorde al Decreto 1499 de 2017, designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área que haga parte de la Alta Dirección. Para las entidades cabeza de sector, el Responsable de Seguridad Digital será el enlace sectorial. Así mismo, debe pertenecer e informar a la Mesa de Trabajo de Seguridad y Privacidad de la Información todo lo referente al SGSI y MSPI, al cual asistirá en forma oportuna y garantizará el mejoramiento continuo de cualquier necesidad de mejora respecto a la seguridad y privacidad de la información del Ministerio.

- De otra parte, tendrá la responsabilidad de liderar a la Mesa de Trabajo de Seguridad y Privacidad de la Información y desarrollará las siguientes funciones (además de las determinadas en la resolución 4-0362 de 2017):
- Emitir conceptos referentes a riesgos y seguridad de la información de la entidad, para la toma de decisiones por parte de la Mesa de Trabajo de Seguridad y Privacidad de la Información.
- Coordinar la implementación, despliegue y sostenibilidad del SGSI y MSPI.
- Mantener una comunicación clara, oportuna, completa y permanente con los integrantes de la Mesa de Trabajo de Seguridad y Privacidad de la Información.
- Definir las herramientas, metodologías y lineamientos necesarios para la implementación del SGSI y MSPI.
- Realizar seguimiento a los objetivos planteados frente al SGSI y MSPI, para detectar desviaciones y tomar las acciones correctivas necesarias.
- Verificar el cumplimiento de la implementación de los objetivos y tareas asignadas a la Mesa de Trabajo de Seguridad y Privacidad de la Información.
- Verificar que se incluyan los temas asociados al SGSI y MSPI, dentro del plan de capacitaciones de la entidad.
- Asegurar que se definan e implementen actividades de sensibilización y concienciación frente a la seguridad de la información a la Alta Dirección y demás partes interesadas.
- Emitir conceptos y asesoría sobre los temas de seguridad de la información al Comité de Seguridad de la información para la toma de decisiones.
- El Oficial de Seguridad de la Información o quien haga sus veces definirá las opciones mínimas requeridas para la protección, configuraciones aceptables e instalación de antivirus para de los dispositivos móviles de la entidad.



5.2.3. Mesas de trabajo de seguridad y privacidad de la información

Las Mesas de Trabajo de Seguridad y Privacidad de la Información garantizarán el apoyo y toma de decisiones al proceso de definición, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI, el SGCN y en consecuencia el MSPI a través de un equipo de trabajo conformado y con funciones determinadas en la resolución 4-0362 de 2017.

5.2.4. Responsable de los riesgos de seguridad de la información

Todos los funcionarios de MINENERGÍA serán responsables de la identificación, evaluación y control de los riesgos de seguridad de la información.

No obstante, el Ministerio debe asignar un responsable de la administración, custodia y preservación lógica o física de los activos de información, de los riesgos de seguridad y privacidad de la información de cada proceso.

Las principales responsabilidades de este rol incluyen, pero no se limitan a:

- Identificar, registrar y actualizar los activos de información de su dependencia o proceso de responsabilidad del MINENERGÍA.
- Realizar la clasificación y valorización de los activos de información y revisarla como mínimo anualmente para garantizar que corresponde a los requisitos legales, normativos, contractuales y de la entidad.
- Revisar y gestionar para que los controles de seguridad sean implementados de acuerdo al nivel de clasificación de la información de su proceso.
- Determinar los privilegios de acceso y criterios de respaldo para los activos de información bajo su responsabilidad.
- Revisar y asegurar que los privilegios de acceso a los activos de información de los cuales es responsable son los adecuados.
- Aprobar la divulgación de información que este bajo su proceso.
- Comunicar violaciones de seguridad o incidentes sobre los activos de información de su proceso.
- Garantizar que la información que le ha sido confiada sea protegida durante todo su ciclo de vida (creación, almacenamiento, distribución, transporte y destrucción segura) de modificaciones y usos no autorizados.

5.2.5. Responsabilidades de las partes interesadas

Las partes interesadas en sus funciones y roles dentro del MINENERGÍA tienen autorización y acceso a la información y/o activos provenientes del responsable o líder del proceso, dentro de las cuales se incluyen:



- Cumplir con todas aquellas responsabilidades que han sido definidas en las políticas de seguridad del MINENERGÍA.
- Proteger la información que la entidad le ha suministrado para la ejecución de sus labores.
- Firmar un acuerdo de confidencialidad y/o no divulgación antes de iniciar formalmente sus labores dentro de la entidad.
- Firmar aceptación sobre el entendimiento de las políticas, procedimientos, manuales y formatos de seguridad del SGSI y MSPI de la entidad.
- Reconocer que la propiedad intelectual sin limitantes, patentes, derechos de autor, marcas registradas y todos los otros derechos de propiedad intelectual tal como se manifiestan en memorandos, planes, estrategias, productos, programas de computación, documentación y demás material desarrollado o concebido mientras esté desarrollando sus labores o gestión en sitios alternativos de trabajo, son de exclusividad de la entidad.
- Cumplir con las políticas de seguridad y privacidad de la Información definidas por el MINENERGÍA.
- Usar los activos de información de la entidad y los recursos de manera segura y adecuada para desempeñar sus funciones laborales que le son aprobadas previamente.

5.2.6. Responsabilidades de proveedores

Es responsabilidad de todos los proveedores, que tengan acceso a la información del MINENERGÍA, cumplir con todas las políticas y procedimientos definidos frente a la protección de la información, las cuales le han sido suministrados para la labor designada y así mismo usar de manera segura los activos de información que le fueran asignados.

Estos proveedores deben estar autorizados por el responsable o líder del proceso, quien será el gestor del control y vigilancia del uso adecuado de los activos de información.

Los proveedores deben aceptar por escrito los términos y condiciones de uso de los activos de información, así como el cumplimiento estricto de las políticas de seguridad de la información del MINENERGÍA antes de su acceso a los mismos.

5.2.7. Analista seguridad de la información

- Guiar a la Alta dirección del Ministerio ante incidentes de seguridad mediante el plan de respuesta de incidentes.
- Responsable de proponer y coordinar la realización del análisis de riesgos de seguridad de la información.
- Responsable de la elaboración y desarrollo del Plan de Seguridad de la Información.
- Mantener contacto con grupos de interés.
- Mantener y promover la actualización de las políticas de seguridad de la información.
- Debe responder por la revisión de problemas de seguridad de la información existentes y aquellos que se consideren potenciales.



5.2.8. Grupo de Infraestructura Tecnológica:

- El Grupo de Infraestructura Tecnológica debe activar la opción de cifrado para los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.
- El Grupo de Infraestructura Tecnológica debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos y restaurar los valores de fábrica de manera remota, para evitar divulgación no autorizada de información en caso de pérdida o hurto.
- El Grupo de Infraestructura Tecnológica debe garantizar las copias de seguridad de la información contenida en los dispositivos móviles institucionales.
- El Grupo de Infraestructura Tecnológica creará, modificará, bloqueará o eliminará las cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información de la entidad, acorde con el procedimiento establecido por el SGSI y según solicitud por escrito de las partes interesadas.
- El Grupo de Infraestructura Tecnológica realizará los cambios necesarios a los roles y perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos de acuerdo a solicitud escrita de las partes interesadas.
- El Grupo de Infraestructura Tecnológica, gestionará los incidentes de seguridad de la información.
- Grupo de Infraestructura Tecnológica, evaluará y autorizará la instalación, cambio o eliminación de componentes de la plataforma tecnológica y los sistemas de información de la entidad.
- El Grupo de Infraestructura Tecnológica garantiza que la implementación de los cambios se lleve a cabo sin generar discontinuidad de la operatividad y la alteración de los procesos para el cumplimiento de la misión institucional.
- El Coordinador del Grupo de Infraestructura Tecnológica debe asegurarse de que todos los funcionarios y/o servidores públicos, contratistas del Grupo de Infraestructura Tecnológica y los líderes funcionales de los servicios de TIC del MINENERGÍA, como también los proveedores que cumplen una función en la gestión de la continuidad de la operación de TIC, estén familiarizados con esta política.

5.6. GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

La realización de un inventario y clasificación de activos hace parte de una administración de la seguridad y privacidad de la información efectiva dentro de una organización y contribuye al cumplimiento del control del Anexo A del estándar ISO/IEC 27001:2013 (inventario de activos, propiedad de activos, clasificación de la información, etiquetado y manipulado de la información).

En el MINENERGÍA, el área encargada de realizar, actualizar, hacerle seguimiento y control al Inventario de Activos de Información es el Grupo de Gestión de la Información y Servicio al Ciudadano (GGISC).

Los activos de información involucrados en todos los procesos de la entidad son propiedad del Ministerio de Minas y Energía y se proporcionan a los funcionarios, servidores públicos, contratistas y proveedores, para cumplir con el propósito de la función pública.

5.6.1. Definición

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

- Número consecutivo único que identifica al activo en el inventario.
- Proceso al que pertenece el activo.
- Propietario / Responsable
- Custodio.
- Nombre del activo de información.
- Descripción del activo de información.
- Categorización del activo de información: por ejemplo, hardware, software, servicio, personas, la cual debe revisarse periódicamente o cuando se presenten cambios en la información o en la estructura que puedan afectarla.
- Idioma.
- Medio de conservación.
- Periodicidad o de generación o actualización en caso de activos expedientes físicos y digitales.
- Condición legítima de la excepción (Ley 1712 transparencia y Ley 1581 tratamiento de datos).
- Fundamento constitucional o legal.
- Descripción de Condición legítima de la excepción.
- Clasificación del activo de acuerdo a la ley de transparencia.
- Valoración del activo (confidencialidad, integridad y disponibilidad).

5.6.2. Revisión

El inventario de activos puede ser revisado o validado en cualquier momento que se requiera y por lo menos debe revisarse y actualizarse una vez al año, con el fin de validar el estado del activo, el proceso al que pertenece, cambio o aumento de actividades, desaparición de un área o proceso, cambios o migraciones de sistemas de información del proceso entre otros.

El Ministerio de Minas y Energía a finales de 2017 y principios de 2018 realizó la actualización del inventario de activos de la información en todos los procesos.

5.6.3. Actualización

Cuando el Ministerio defina alguno de los cambios mencionados anteriormente en los activos de información, debe actualizar el inventario de activos de información.

5.6.4. Publicación

El Ministerio de Minas y Energía, determina que el inventario de activos de información es un documento clasificado como “Público”, sin embargo, aquellos activos de información que por su carácter reservado y que son de naturaleza sensible a los procesos estratégicos de la Entidad, serán clasificados como “Confidenciales”, por lo cual no serán publicados.

El líder de cada proceso será el responsable del inventario de activos de seguridad de la información y las modificaciones que se requieran solo se deben hacer previa autorización del Oficial de Seguridad de la Información o quien haga sus veces.

5.7. PROTECCIÓN DE DATOS PERSONALES

La información es el activo más importante en la actualidad, por tal razón el 17 de octubre de 2012 el Gobierno Nacional expidió la Ley Estatutaria 1581 de 2012 que establece las disposiciones generales para la protección de datos personales, donde se regula el derecho fundamental de hábeas data y se señala la importancia en el tratamiento de la información. La nueva ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación (tratamiento) por parte de entidades de naturaleza pública y privada.

El Ministerio de Minas y Energía en cumplimiento de la Ley cuenta con una política de protección de datos la cual está aprobada y publicada en el Portal WEB.

Adicionalmente, se desarrolló un manual de protección de datos como una herramienta para el tratamiento de los datos de los usuarios y/o titulares el cual está en proceso de revisión.

5.8. CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

El Ministerio de Minas y Energía, buscando dar cumplimiento a la ley y a las mejores prácticas estipuladas en los estándares de las normas 27001:2013, ISO 27002, e ISO 27005 relacionados con la Gestión de Activos ha clasificado los activos de la siguiente manera:

5.8.1. Clasificación de acuerdo con la confidencialidad

Alineados con los tipos de información declarados en la ley 1712 del 2014, el Ministerio de Minas y energía clasificó su información como se describe en la siguiente tabla:

<p>INFORMACION PÚBLICA RESERVADA</p>	<p>Información disponible sólo para un proceso de la Entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.</p>
---	--

INFORMACION PUBLICADA CLASIFICADA	<p>Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta.</p> <p>Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.</p>
INFORMACION PÚBLICA	<p>Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.</p>
NO CLASIFICADA	<p>Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información pública reservada.</p>

Tabla 2: Clasificación por confidencialidad Fuente: Guía para la Gestión y Clasificación de Activos de Información MINTIC

5.8.2. Clasificación de acuerdo con la integridad y disponibilidad

	Disponibilidad	Integridad	Confidencialidad
1 MÍNIMO	<p>La no disponibilidad de la información puede afectar la operación normal de la entidad. No tiene implicaciones legales, económicas o de pérdida de imagen para el Ministerio</p>	<p>Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para el Ministerio.</p>	<p>Es la información que ha sido calificada como de conocimiento público. El conocimiento o divulgación no autorizada de la información no tiene ningún impacto negativo en los procesos del Ministerio.</p>
2 BAJO	<p>La no disponibilidad del activo de información no tiene ningún impacto negativo en los procesos del Ministerio.</p>	<p>La pérdida posible de en la exactitud de algún dato o estado completo de la información puede tener algún impacto negativo en los procesos del Ministerio.</p>	<p>Esta información puede ser entregada o publicada con ciertas restricciones sin que implique daños ni impactos negativos a terceros ni a las actividades y procesos del Ministerio.</p>
3 MEDIO	<p>La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de</p>	<p>Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado al Ministerio.</p>	<p>Es la información que es utilizada por los funcionarios del Ministerio para realizar sus labores en los procesos y que puede ser conocida por terceros con la autorización del propietario del activo. La divulgación no autorizada de la información</p>

	Disponibilidad	Integridad	Confidencialidad
	imagen moderado al Ministerio.		impacta negativamente al proceso evaluado y/u otros procesos del Ministerio.
4 ALTO	La falta o no disponibilidad parcial de la información impacta negativamente la prestación de servicios de tecnología y de información del Ministerio.	La pérdida en la exactitud de algún dato impacta negativamente la prestación de servicios de tecnología y de información en el Ministerio de Minas.	La divulgación no autorizada de la información impacta negativa y significativamente al proceso evaluado y/u otros procesos del Ministerio
5 CRITICO	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.	A esta información sólo pueden tener acceso las personas que expresamente han sido declaradas usuarios legítimos de esta información, y con los privilegios asignados. La divulgación no autorizada de esta información impacta negativamente al Ministerio.

Tabla 3 Esquema de calificación por disponibilidad, integridad y confidencialidad Fuente el autor

5.9. ETIQUETADO DE ACTIVOS DE INFORMACIÓN

Con el propósito de mantener una apropiada protección de los activos de información del Ministerio de Minas y Energía, se han generado políticas de clasificación y etiquetado de acuerdo a la norma ISO 27001, las cuales deben ser cumplidas por todas las partes interesadas, con el fin de no exponer al Ministerio a riesgos innecesarios.

5.10. GESTIÓN DOCUMENTAL DEL MSPI

Actualmente el Ministerio de Minas y Energía, se encuentra certificado en Calidad, con la ISO 9001:2008, por lo tanto, se aplica los procedimientos existentes para el control documental del MSPI, y cuenta con un sistema de información SIGME para establecer los documentos los procesos, caracterizaciones, mapas de riesgos, objetivos e indicadores de gestión y demás temas.

5.10.1. Ventajas de la integración

Las ventajas de la integración son las siguientes:



- Se evita duplicar esfuerzos ya que hay varios puntos en común, por ejemplo, el procedimiento que, definido para controlar los documentos y registros relacionados, con el Sistema de Gestión de Calidad, se puede utilizar perfectamente para los documentos que se desprendan del MSPI.
- Además de la gestión de la documentación, las auditorías internas se pueden planificar conjuntamente, el Informe de Revisión por la Dirección se puede unificar para que un único documento recoja las exigencias de todas las normas, el tratamiento de las No Conformidades y las Mejoras se pueden abordar de igual forma independientemente de la norma específica de la que desprendan, entre otros.
- Si se integra el Sistema de Gestión de Seguridad y Privacidad de la Información, el MSPI y el SGC, facilitará tanto la comunicación como las sinergias entre los procesos del Ministerio de Minas y energía.

5.10.2. Creación y actualización de documentación

Para la creación y actualización de la documentación en el Ministerio de Minas y Energía, debe incluirse lo siguiente:

- Información descriptiva: título, versión, fecha y codificación.
- Control de cambios entre versiones.
- Etiquetado y clasificación de la información del documento.
- Firma de quien elaboró, quien revisó y quien aprobó.

Lo anterior se enmarca en lo definido en el procedimiento para el Control de los Documentos identificado con el código AG-P-02 del Ministerio de Minas y Energía publicado en el aplicativo web SIGME.

5.10.3. Control de la información documentada

El Ministerio de Minas y Energía cuenta con seis (6) repositorios oficiales de documentación, como son: La página web, el correo electrónico, el sistema de información SIGME, sistema de información P8, carpetas compartidas y archivo físico en cada proceso de la entidad. Estos repositorios deben cumplir con las siguientes características que permitirán asegurar la confidencialidad, integridad, disponibilidad y privacidad de la información:

- Acceso continuo a la información a través del sistema de Información SIGME, donde se encuentra protegida en formato de lectura PDF o formato de imagen.
- Transmisión de información entre el usuario y el servidor a través de protocolos seguros, que permite garantizar la confidencialidad de la información.
- La administración y control de los documentos del MSPI, debe continuar a cargo de la Oficina de Planeación, tal como ocurre para el Sistema de Gestión de Calidad SGC existente.



- Desde los sistemas de información del Ministerio de Minas y Energía, se otorgan los permisos de acceso y/o modificación de la información documentada a las partes interesadas.
- Los permisos de acceso los debe aprobar previamente el Oficial de Seguridad de la Información o quien haga sus veces de la entidad para el caso del MSPI.
- Algunos documentos del MSPI serán clasificados como confidenciales (reservados o clasificados), los cuales no se podrán tener acceso para el público en general, únicamente se tendrá acceso desde las instalaciones del Ministerio y los cuales llevarán una contraseña para su apertura y lectura.

En relación con la información documentada de origen externo, se define en el procedimiento antes mencionado como leyes, decretos, resoluciones, circulares reglamentarias emitidas por otras entidades necesarias para el desarrollo de los procesos, se integrará igual como se maneja actualmente por el área de calidad ISO 9001:2008 del Ministerio de Minas y Energía, en el “Listado Maestro de Documentos”, evidenciando que es del MSPI.

En el caso de los registros, definidos como documentos que presentan los resultados obtenidos o evidencia de actividades realizadas, el Ministerio de Minas y Energía, ha establecido los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de retención y la disposición de los registros que le permitan la recuperación de la información y la preservación de la memoria institucional de la entidad con el procedimiento Control de Registros GD-P-01 publicado en el aplicativo SIGME y sus respectivas tablas de retención documental.

5.11. GESTIÓN DE RIESGOS

De acuerdo con la norma técnica ISO 31000, se define el riesgo como “el efecto de la incertidumbre sobre los objetivos” (ISO31000 Icontec, 2011, Pág.4). El objetivo general de la norma es brindar principios y directrices genéricos para gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información.

La Gestión para los riesgos asociados a la seguridad y privacidad de la información y el MSPI del Ministerio de Minas y Energía se ha basado en las recomendaciones de la norma ISO 27000, la “Guía de Riesgos” del DAFP y la Guía de gestión de riesgos del Modelo de Seguridad y Privacidad de la información MSPI, buscando que haya una integración a lo que se ha desarrollado dentro de la Entidad para otros modelos de Gestión.

Así mismo, para la evaluación de riesgos en seguridad de la información el Ministerio ha clasificado sus activos de información por proceso a los cuales se les ha identificado los riesgos teniendo en cuenta que la Entidad debe preservar la Confidencialidad, Integridad y Disponibilidad de la información.

Para lograr la confidencialidad, integridad y disponibilidad de la información el Ministerio ha determinado que el apetito del riesgo de seguridad de la información es bajo.

5.11.1. Incidentes de la seguridad de la información

De acuerdo con la norma ISO 27001:2013 un incidente de seguridad de la información está definido como “un evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen la probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información” (ISO27001 Icontec, 2013). A continuación, se mencionan algunos de los siguientes incidentes que pueden llegar a suceder en el Ministerio de Minas y Energía:

- Acceso no autorizado a la información.
- Divulgación de información sensible.
- Denegación del servicio.
- Daño de la información.
- Ataques externos o internos.
- Pérdida o robo de la información.
- Modificación no autorizada.
- Diligenciamiento errado de formatos.
- Perdida o daño de la documentación.

5.11.2. Eventos

De acuerdo la NTC ISO 27001:2013, se define un evento de seguridad de la información como “la presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.” (ISO 27001:2013, ICONTEC, Pág. 11, 2013), a continuación, se mencionan algunos de los eventos de seguridad de la información que se pueden afectar al Ministerio de Minas y Energía:

Evento	Descripción
Fraude Interno	Está asociado a la intención por parte de un funcionario de la organización de obtener información con fines ajenos a su labor.
Fraude Externo	Son actos realizados por personas externas a la organización, que buscan apropiarse indebidamente de la información, por medio de acceso no autorizado, alterando o vulnerando el procesamiento de la información.
Clientes	Según el Anexo A.9.2.2. de la norma ISO 27001:2013 “Se debe implementar el suministro de acceso formal de usuarios para asignar o revocar los accesos para todo tipo de usuario”
Fallas Tecnológicas	Pérdida de información asociada a fallas tecnológicas debido a fallas en el procesamiento de la información que

Evento	Descripción
	vulneran la confidencialidad, integridad y disponibilidad de esta.
Ejecución y administración de procesos	Pérdida de información asociada a errores de administración y ejecución de procesos.

Tabla 4 Eventos asociados al SGSI Fuente: Anexo A de la norma ISO 27001:2013

5.12. VISIÓN GENERAL PARA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Proceso para la administración del riesgo en seguridad de la información.

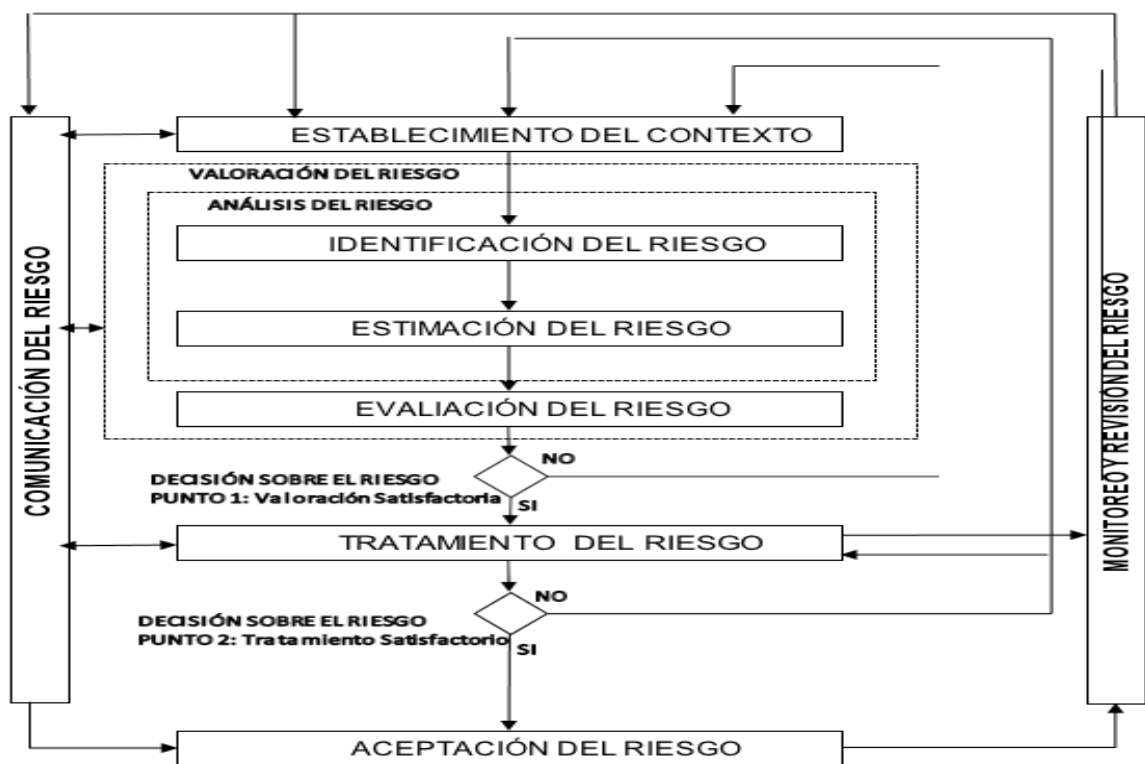


Ilustración 1: Proceso para la administración del riesgo en seguridad de la información.

Tomado de la NTC-ISO/IEC 27005 Fuente Guía de gestión de riesgos MINTIC

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI.

ETAPAS DEL MSPI	PROCESO DE GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN
Planear	<ul style="list-style-type: none"> • Establecer Contexto. • Valoración del riesgo. • Planificación del Tratamiento del riesgo. • Aceptación del riesgo.
Implementar	<ul style="list-style-type: none"> • Implementación del plan de tratamiento de riesgo
Gestionar	<ul style="list-style-type: none"> • Monitoreo y revisión continuo de los riesgos
Mejora Continua	<ul style="list-style-type: none"> • Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información.

Tabla 5 Etapas de la Gestión del Riesgo a lo Largo del MSPI-Fuente Guía de gestión de riesgos MINTIC

5.12.1. Establecimiento del contexto

El Ministerio de Minas y Energía, es consciente de la necesidad de conocer y comprender su contexto externo e interno y como éste puede impactar de forma positiva o negativa el cumplimiento de sus objetivos y en este caso Confidencialidad, Integridad y Disponibilidad de la información.

5.12.2. Contexto interno y externo

En este contexto se contemplan las condiciones internas y externas del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos del Ministerio de Minas y Energía, este contexto determina los elementos, subsistemas y condiciones en que se desenvuelve la Entidad, el comportamiento organizacional y aquello que tiene un impacto en el Ministerio, tales como la misión, visión, historia, organigrama, objetivos del Ministerio, función del Ministerio entre otros, los cuales están consignados en el sistema integrado de gestión cuya conformación está dada por los Sistemas de Control Interno, Gestión de la Calidad y Desarrollo Administrativo y se encuentran publicadas en la página web.

5.12.3. Valoración de los riesgos

Para la valoración de los riesgos se tienen en cuenta los siguientes aspectos:

Una vez identificados los activos de información, la Oficina de Planeación y Gestión Internacional, deberá proceder a la identificación de los riesgos en cada uno de los procesos del Ministerio de Minas y Energía:

Estratégicos:

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

Misionales:

- Formulación y adopción de políticas, planes, programas, reglamentos y lineamientos sectoriales.
- Ejecución de políticas, proyectos y reglamentación sectorial.
- Seguimiento, vigilancia y control a políticas, planes, programas, proyectos y reglamentación sectorial.

Apoyo:

- Gestión del talento humano.
- Gestión documental.
- Gestión financiera.
- Gestión tecnológica, de información y comunicación.
- Gestión de recursos físicos.
- Gestión Jurídica.

Evaluación y control:

- Auditoría y evaluación
 - Control disciplinario.
1. Se enumera el riesgo, para dar un orden consecutivo de los riesgos de seguridad de la información.
 2. Se identifica el riesgo: con el fin de determinar que podría suceder que cause una pérdida potencial, de la confidencialidad, integridad y disponibilidad de la información. Se realiza una descripción clara de los riesgos de seguridad de la información.
 3. Se determina los criterios de impacto, que son las consecuencias que puede ocasionar al Ministerio la materialización del riesgo.

Es de anotar que el valor del impacto para los riesgos de seguridad y privacidad de la información, resultan de promediar los diferentes impactos establecidos en la siguiente tabla:

CATEGORIA	VALOR CATEGORIA	IMPACTO DE CONFIDENCIALIDAD	IMPACTO DE CREDIBILIDAD O IMAGEN	IMPACTO LEGAL	IMPACTO OPERATIVO
LEVE	1	Personal	Grupo de funcionarios	Multas	Ajustes a una actividad concreta.
MENOR	2	Grupo de trabajo	Todos los funcionarios	Demandas	Cambios en los procedimientos.
MODERADO	3	Relativa al proceso	Usuarios ciudad	Investigacion Disciplinaria	Cambios en la interaccion de los procesos.
ALTO	4	Institucional	Usuarios region	Investigacion Fiscal	Intermitencia en el servicio.
CATASTROFICO	5	Estrategica	Usuarios pais	Intervencion - Sancion	Paro total del Proceso.

Ilustración 2 : Clasificación por confidencialidad

4. Se determinan los criterios de probabilidad de ocurrencia de cada uno de los riesgos, probabilidad de la posibilidad de ocurrencia del riesgo y su calificación esta dado de acuerdo con los parámetros de la siguiente tabla:

CATEGORIA	VALOR CATEGORIA	DESCRIPCION	FRECUENCIA
RARO	1	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
IMPROBABLE	2	El evento puede ocurrir en algún momento	Al menos de una vez en los últimos 5 años.
POSIBLE	3	El evento podría ocurrir en algún momento	Al menos de una vez en los últimos 2 años.
PROBABLE	4	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de una vez en el último año.
CASI SEGURO	5	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año.

Ilustración 3: Criterios de probabilidad

5. Se valora el riesgo inherente el riesgo al cual se está expuesto sin ningún tipo de control sobre el activo. Para valorar el riesgo inherente, se asignan las siguientes calificaciones: impacto financiero (IF), impacto reputacional (IR), impacto operativo (IO), impacto legal (IL) y probabilidad (PR). Al asignar las calificaciones al riesgo inherente se debe considerar que el activo no cuenta con controles para mitigar el impacto o reducir la probabilidad.

El valor del riesgo inherente se obtiene al aplicar la siguiente fórmula:

$$(1) RI = (IC + IR + IO + IL) * PR$$

Riesgo Inherente

(IF:	2	+	IR:	3	+	IO:	4	+	IL:	4)	X	PR:	3	=	RIESGO:	39
------	---	---	-----	---	---	-----	---	---	-----	---	---	---	-----	---	---	---------	----

Figura No. 5. Cálculo del riesgo inherente

6. Se realiza la evaluación de los controles establecidos para mitigar los riesgos: La evaluación de los controles se realiza cuando se ha establecido el riesgo inherente en cada uno de los procesos. Es importante anotar que el Ministerio cuenta con una declaración de aplicabilidad en la cual se contemplan los controles correspondientes al Anexo A de la norma NTC: ISO/IEC 27001.

La evaluación de controles se realiza de la siguiente manera:

- Identificación de los controles relacionados a cada uno de los riesgos establecidos.
 - Es necesario establecer si el control es preventivo (reducen probabilidad).
 - Es necesario establecer si el control es correctivo (reduce impacto).
 - Se determina:
 - Efectividad
 - Implementación
 - Solidez
 - Finalmente, la calificación del control determina el desplazamiento o no del riesgo en sus niveles de impacto y probabilidad, dependiendo, entre otros aspectos, de si los controles disminuyen o no los niveles de probabilidad e impacto obtenidos en el riesgo inherente.
 - Una vez evaluados los controles se determina el riesgo residual sobre el cual se realizará el plan de tratamiento.
7. Planificación del Tratamiento del riesgo: Una vez se obtienen los resultados del análisis de los riesgos de seguridad y privacidad de la información, se gestionan los riesgos residuales, se proponen acciones de mejora a través de planes de acción o de tratamiento, con la finalidad que la información siempre conserve las características de confidencialidad, integridad y disponibilidad de esta.

Para definir y desarrollar los planes de acción o tratamiento de los riesgos a tratar se deben tener en cuenta las siguientes apreciaciones:

- Si se encuentra en una zona de aceptación o apetito de riesgo (bajo) los riesgos son aceptados y monitoreados por lo menos dos veces al año.
- Son susceptibles de ser tratados los riesgos residuales de seguridad de la información que se encuentren en una zona moderada hacia arriba, para dicho tratamiento se deben contemplar la implantación de un nuevo control o fortaleciendo los ya existentes.

- Si la decisión es aceptar el riesgo residual de seguridad y privacidad de la información, independiente de donde se encuentre ubicado y la afectación que pueda tener para confidencialidad, integridad y disponibilidad de la información, se deben hacer revisiones por lo menos cada dos meses tanto de los riesgos como de los controles que puedan tener.
- Si la decisión del Ministerio ante el riesgo residual de seguridad y privacidad de la información es transferirlo, se deberá realizar un análisis de costo beneficio correspondiente con el fin de determinar la viabilidad de la transferencia.

5.12.4. Seguimiento y monitoreo del Sistema de Gestión de Seguridad y Privacidad de la Información y del MSPI:

El Ministerio de Minas y Energía, evaluará el desempeño y la eficacia del Sistema de Gestión de Seguridad y Privacidad de la Información y el MSPI contra las políticas, los objetivos y la experiencia práctica de la gestión de seguridad de la información, a la vez que se reportan los resultados a la dirección para su revisión y toma de decisiones.

El Ministerio debe realizar las siguientes actividades de monitoreo:

- Monitorear la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- Monitorear periódicamente la evaluación de los riesgos desarrollada en la entidad, donde a su vez se validen los niveles aceptables del riesgo residual después de la aplicación de controles y medidas administrativas.

El Ministerio de Minas y Energía debe conservar información documentada apropiada como evidencia de los resultados del monitoreo y la medición.

5.12.5 Auditorías internas.

El Ministerio de Minas y Energía, No programa y ejecuta auditorías internas con fechas planificadas, tal como lo establece la norma ISO 27001:2013 y el plan de auditoría de la Entidad.

5.12.6 Revisión por parte de la alta dirección.

El Ministerio de Minas y Energía realiza periódicamente la respectiva revisión por parte de la Alta Dirección según lo establecido en la norma ISO 27001:2013.

5.13. MEJORA CONTINUA DEL SGSI

Una vez realizado el seguimiento, evaluación, análisis y monitoreo al Sistema de Seguridad y Privacidad de la Información, es necesario, desarrollar un proceso de mejoramiento continuo, el cual le permitirá al Ministerio, corregir errores cometidos, mejorar las acciones llevadas a cabo en las fases anteriores.

Para lograr la mejora continua se deben tener en cuenta las siguientes consideraciones:

- Cuando existan no conformidades, el proceso correspondiente debe llevar a cabo las acciones para mitigar el impacto de su existencia.
- Se revisan las no conformidades para disminuir o eliminar las causas y consecuencias que estas puedan generar, y evitar que se presente nuevamente.
- Se determinan si existen otras no conformidades similares para establecer acciones preventivas evitando su materialización.
- Empezar acciones detectivas que permitan gestionar el riesgo a tiempo, disminuyendo el impacto y la probabilidad de ocurrencia.
- Llevar un registro en el sistema de información que determine el Ministerio a los tratamientos realizados y a las no conformidades, así como las acciones realizadas para mitigar el impacto.

5.13.1. Aseguramiento del Protocolo IPv6

El Ministerio de Minas y Energía, siguiendo los lineamientos del MINTIC está realizando la transición del protocolo IPv4 a IPv6, en su contexto ha tomado como base las características de confidencialidad, integridad, disponibilidad y privacidad de la información; a fin de generar mecanismos de direccionamiento IP de acceso seguro y uso eficiente de las infraestructuras de información y comunicación para proteger los bienes, activos, servicios, derechos y libertades del Ministerio.

5.13.2. Gestión y Clasificación de Incidentes de Seguridad de la Información.

Se establece para el Ministerio de Minas y Energía un procedimiento y un formato para gestionar los eventos de seguridad de la información con el fin de detectarlos, tratarlos con eficiencia y estandarizar las actividades a seguir para su atención y manejo.

El objetivo principal es estructurar la administración adecuada de los incidentes de seguridad, de tal manera que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de una base registros de incidentes que permitan generar indicadores, establecer posibles riesgos, a continuación, presentamos un catálogo de las acciones que son consideradas incidente.

Categoría		Acciones no autorizadas
Subcategorías		
1	Acceso lógico no autorizado (sistemas o redes).	
2	Acceso físico no autorizado (equipos, zonas restringidas).	
3	Cambio de privilegios de sistema sin autorización.	
4	Cambio o adición de software sin autorización.	



5	Copia no autorizada o robo de Software.
6	Descarga o envío de contenido inapropiado.
7	Instalación de Software no autorizado.
8	Modificación o inserción de transacciones, archivos o bases de datos sin autorización.
9	Procesamiento ilegal de datos.
10	Modificación o manipulación no autorizada del Hardware.
11	Uso de software no licenciado.
12	Piratería de Software.
13	Uso inadecuado de activos o sistemas para generar fraudes.
14	Uso inadecuado de activos o sistemas que generan interrupción.
15	Almacenamiento y/o transferencia de archivos o aplicaciones contaminados.
16	Acceso a sitios web Restringidos y/o No Autorizados.
17	Divulgación no autorizada de Credenciales de autenticación.
18	Compartir archivos sensibles o con datos personales.
19	Consumo Excesivo de Canal.
Categoría	
Compromiso de la Información / Servicios	
Subcategorías	
1	Actividades de ingeniería social.
2	ANS / OLA inefectivos o desactualizados.
3	Cracking de contraseñas.
4	Cracking de llaves.
5	Datos provenientes de fuentes no confiables.
6	Denegación de servicio.
7	Desfiguración de página web.
8	Distribución de spam.
9	Distribución de virus de computador.
10	Divulgación de información (negocio, clientes, personal o privada).
11	Ejecución de pruebas maliciosas o escaneos.
12	Escucha encubierta (Eavesdropping).
13	Espionaje.
14	Hacking.
15	Introducción de código malicioso.
16	Introducción de troyanos.
17	Mala práctica en la evaluación y selección de proveedores.
18	Modificación de tráfico de red.
19	Recuperación de medios reciclados o desechados.
20	Robo de equipo de cómputo.



21	Robo de información, medios o documentos (negocio, clientes, personal o privada).
22	Suplantación de identidad de usuarios.
23	Suplantación de sitios web.
Categoría	
Compromiso de las Funciones	
Subcategorías	
1	Dependencia de Servidores Públicos críticos.
2	Dependencia de Proveedores o Terceros.
3	Abuso de derechos.
4	Cambios imprevistos en equipos de cómputo o comunicaciones.
5	Cambios imprevistos en procesos de usuarios o instalaciones.
6	Procedimientos no documentados.
7	Cambios imprevistos en el Software.
8	Cambios imprevistos en la estructura organizacional.
9	Cambios imprevistos en la información de negocio.
10	Incumplimiento de ciclos de mantenimiento.
11	Efectos imprevistos en la introducción de procesos de negocio nuevos o modificados.
12	Mala distribución del área o diseño del puesto de trabajo.
13	Falta de orden y aseo.
14	Nivel de exigencia alto para el desarrollo de las tareas (contenido de la tarea).
14	Relaciones humanas conflictivas (trabajo solo, excesiva supervisión, dificultad relación con otros compañeros y jefes).
16	Inadecuada organización de tiempo de trabajo.
17	Turnos de trabajo inadecuados.
18	Mala práctica en la evaluación y selección de proveedores.
Categoría	
Daño Físico	
Subcategoría	
1	Accidentes (aeronave, automotor, motonave, ferroviario).
2	Caída de objetos desde niveles superiores.
3	Contaminación (aire, agua, tierra).
4	Explosiones (nube de vapor, sobrepresión, polvos /fibras, termodinámicas).
5	Falla estructural.
6	Incendio (estructural, climáticos, líquidos inflamables, gases inflamables).
7	Instalaciones y estructuras deficientes, aberturas en el piso.
Categoría	
Eventos Naturales	
Subcategoría	
1	Biológica (plaga, pandemia, ingestión de alimentos contaminados, virus y bacterias).



2	Climática (vendaval, huracán, granizada, sequia, helada, inundación, descargas atmosféricas).
3	Geológica (sismo, deslizamiento, erupción volcánica, maremoto).
4	Inundación.
Categoría	
Fallas Técnicas	
Subcategoría	
1	Daño eléctrico.
2	Daño o pérdida de equipos e instalaciones de cómputo.
3	Deterioro de equipos.
4	Falla Hardware.
5	Falla Software.
6	Malfuncionamiento de computadores o equipos de red.
7	Malfuncionamiento de las aplicaciones de Software o equipos de terceros.
8	Malfuncionamiento de las aplicaciones de Software o equipos de MINENERGÍA.
9	Sobrecarga de sistema.
10	Cargas estáticas.
Categoría	
Perdida de Servicios Esenciales	
Subcategoría	
1	Daño o pérdida de los servicios o enlaces de comunicaciones.
2	Pérdida de energía, agua o aire acondicionado.
Categoría	
Personal	
Subcategoría	
1	Fraude o robo.
2	Accidentes laborales.
3	Competencia desleal.
4	Errores humanos / operación.
5	Falta de compromiso.
6	Huelga.
7	Motín.
8	Paro.
9	Sabotaje.
Categoría	
Perturbación del servicio	
Subcategoría	
1	Radiaciones (ultravioleta).
2	Radiaciones no ionizantes (campos electromagnéticos).
3	Ruido.
4	Temperatura extrema (frio o calor).



5	Vibraciones.	
Categoría		Terrorismo, Narcotráfico, Delincuencia
Subcategoría		
1	Asonadas, Conmoción Civil.	
2	Agresión, asaltos, vandalismo o atentados.	
3	Extorsión o chantaje.	
4	Hostigamiento.	
5	Retención o secuestro.	
Categoría		Otro
Subcategoría		
	No definido en Clasificaciones anteriores.	

Tabla 6: Tabla de categoría y subcategorías de acciones no autorizadas. Fuente: Autor



6. CONCLUSIONES Y RECOMENDACIONES

- 6.1 MINENERGÍA presenta avances en la implementación del SGSI, SGCN y MSPI debido al alto compromiso de gestores del Grupo de Infraestructura Tecnológica, interesados en adoptar las buenas prácticas de seguridad de la información y continuidad del negocio.
- 6.2 Se recomienda el nombramiento oficial del cargo de Oficial de Seguridad de la Información o quien haga sus veces y Continuidad de Negocio, roles que se mencionan y se promueven en la resolución 4-0362 de 2017. Roles de alta importancia ya que según las funciones dadas en la resolución deben dirigir las mesas de trabajo N° 1 de Seguridad y Privacidad de la Información y la mesa de trabajo N° 2 de Gestión del Cambio y Continuidad de Negocio.
- 6.3 Por otro lado, desde septiembre de 2017, se han establecido procedimientos, planes de mejora y métricas que deben ser adoptados e institucionalizados tanto por la Entidad en General como por el Grupo de Infraestructura Tecnológica, pero para esto se requiere un nivel alto de gobierno, por lo cual se recomienda que la Dirección Ejecutiva de las mesas de trabajo, esté a cargo de la Secretaria General.