COLOMBIA POTENCIA DE LA VIDA

Energía

40646

RESOLUCIÓN NÚMERO DE

(01 NOV 2023)

Por la cual se adoptan las políticas aplicables al Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio de Minas y Energía

EL MINISTRO DE MINAS Y ENERGÍA

En ejercicio de las facultades constitucionales y legales, en especial las otorgadas en el artículo 208 de la Constitución Política de Colombia y en particular de las previstas en los artículos 37, 59 y 61 de la Ley 489 de 1998, los artículos 2.2.22.2.1 y 2.2.35.3 del Decreto 1083 de 2015 y el artículo 2.2.21.1.2.1 del Decreto 338 de 8 marzo de 2022, y

CONSIDERANDO

Que el artículo 2 de la Ley 1341 de 2009, modificado por el artículo 3 de la Ley 1978 de 2019, establece que *"La investigación, el fomento, la promoción y el desarrollo de las Tecnologías de la Información y las Comunicaciones son una política de Estado que involucra a todos los sectores y niveles de la administración pública y de la sociedad, para contribuir al desarrollo educativo, cultural, económico, social y político e incrementar la productividad, la competitividad, el respeto a los Derechos Humanos inherentes y la inclusión social. (...)".*

Que de conformidad con el numeral 8 del artículo 2 de la Ley 1341 de 2009 y el principio orientador de *"Masificación del Gobierno en Línea"*, hoy Gobierno Digital, se tiene que, las entidades públicas, con el fin de prestar servicios eficientes a los ciudadanos, deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones y que el Gobierno nacional fijará los mecanismos y condiciones para garantizar el desarrollo de este principio y en la reglamentación correspondiente establecerá los plazos, términos y prescripciones, no solamente para la instalación de las infraestructuras indicadas y necesarias, sino también para mantener actualizadas y con la información completa los medios y los instrumentos tecnológicos.

Que el artículo 2.2.22.2.1 del Decreto 1083 de 2015, Único Reglamentario del Sector Función Pública, establece las Políticas de Gestión y Desempeño Institucional, entre las que encuentran en los numerales 11 y 12, las políticas de Gobierno Digital (antes Gobierno en Línea) y Seguridad Digital respectivamente, las cuales se regirán por las normas que así las regulen o reglamenten y se implementarán a través de planes, programas, proyectos y metodologías y estrategias.

Que el artículo 2.2.35.3 del Decreto 1083 de 2015, adicionado por el Decreto número 415 de 2016, establece que, para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones las entidades y organismos a que se refiere ese Decreto, entre otras, deberán: *"3. Desarrollar los lineamientos en materia tecnológica, necesarios para definir políticas, estrategias y prácticas que habiliten la gestión de la Entidad y/o sector en beneficio de la prestación efectiva de sus servicios y que a su vez faciliten la gobernabilidad y gestión de las Tecnologías de la Información y las Comunicaciones (TIC). Así mismo, velar por el cumplimiento y actualización de las políticas y estándares en esta materia"* y *"11. Desarrollar estrategias de gestión de información para garantizar la pertinencia, calidad, oportunidad, seguridad e intercambio con el fin de lograr un flujo eficiente de información disponible para el uso en la gestión y la toma de decisiones en la Entidad y/o sector"*.

Que el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, dispone que la Política de Gobierno Digital será definida por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, la cual desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC.

Que de conformidad con lo anterior, el Ministerio de Minas y Energía expidió la resolución 40362 de 2017 por medio de la cual se adoptó la Política General de Seguridad y Privacidad de la Información, la política de Tratamiento y Protección de Datos Personales, la Política de

Continuidad del Negocio, la Política de Recuperación ante Desastres TIC y la Política de Seguridad y Privacidad de la Información.

Que el parágrafo del artículo 16 del Decreto ley 2106 de 2019 *"por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública"* señala que las autoridades deberán disponer de una estrategia de seguridad digital, para la gestión documental electrónica y preservación de la información, siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.

Que a través de la Resolución 500 del 10 de marzo de 2021, el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, estableció los lineamientos y estándares para la estrategia de seguridad digital y adoptó el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la política de Gobierno Digital, con el objeto de establecer los lineamientos generales para la implementación del Modelo de Seguridad de la Información (MSPI), la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital, y establecer los lineamientos y estándares para la estrategia de seguridad digital.

Que de conformidad con el artículo 2 de la Resolución 500 de 10 de marzo de 2021, los sujetos obligados a atender los lineamientos fijados en ese acto son los señalados en el artículo 2.2.9.1.1.2 del decreto 1078 de 2015, dentro de los cuales se encuentra esta Cartera Ministerial.

Que en cumplimiento de lo anterior, ante el Comité Institucional de Gestión y Desempeño de este Ministerio se presentó el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos y Seguridad y Privacidad de la Información. Planes que fueron aprobados mediante acta de reunión del 24 de enero de 2022, los cuales requieren ser adoptado mediante la presente resolución.

Que de acuerdo con lo establecido en el numeral 3 de la Directiva Presidencial No. 2 de 24 de febrero de 2022 en la que se insta a las entidades públicas de la rama ejecutiva del orden nacional a *"implementar una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital, de conformidad con el Modelo de Seguridad y Privacidad de la Información (MSPI) dispuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC (…)"* y atendiendo lo dispuesto en el artículo 2.2.21.1.2.1 del Decreto 338 de 8 marzo de 2022, en el que se establece el modelo de gobernanza de la seguridad digital, se hace necesario que el Ministerio de Minas y Energía actualice los lineamientos y el modelo de gobernanza de la seguridad digital institucional adoptados mediante la Resolución 0362 de 2017, de conformidad con las normas vigentes.

Que en mérito de lo expuesto,

RESUELVE

Artículo 1. OBJETO: Adoptar la Política General de la Seguridad y Privacidad de la Información, la Política de Tratamiento y Protección de Datos Personales, la Política de Continuidad del Negocio o del Sistema de Gestión y Continuidad del Negocio, la Política de Recuperación ante Desastres TIC y las Políticas Específicas de Seguridad y Privacidad de la Información en el Ministerio de Minas y Energía, como marco de referencia para el desarrollo de proyectos de tecnología con una gestión eficiente y optimización de los recursos, servicios TIC, y los sistemas de información.

Artículo 2. OBJETIVOS DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN: Son objetivos del modelo de Seguridad y Privacidad de la Información del Ministerio de Minas y Energía los siguientes:

1. Gestionar los riesgos de seguridad y privacidad de la información y seguridad digital.
2. Mitigar los Incidentes de seguridad y privacidad de la información y seguridad digital.
3. Fomentar una cultura de seguridad y privacidad de la información y seguridad digital en el Ministerio, para que todos los colaboradores tomen conciencia de sus deberes y

responsabilidades frente al Sistema General de Seguridad de la Información – SGSI-, al Sistema General de Continuidad del Negocio -SGCN- y el Modelo de Seguridad y Privacidad de la Información – MSPI- adoptando también estrategias y mecanismos de ciberseguridad y ciberdefensa, dentro del marco de las recomendaciones y buenas prácticas de los organismos internacionales y las autoridades competentes en Colombia.
4. Establecer las directrices y lineamientos requeridos para proteger la información y los sistemas de información ante cualquier amenaza que pueda comprometer la confidencialidad, disponibilidad e integridad de esta.

Artículo 3. ÁMBITO DE APLICACIÓN: Las disposiciones que establece el modelo de seguridad y privacidad de la información, sus políticas y lineamientos, aplican a los servidores públicos, contratistas, proveedores y/o terceros usuarios cuando se recolecte, procese, almacene, recupere, intercambie, consulte información y demás, en el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

Artículo 4. POLÍTICAS. La presente resolución adopta las siguientes políticas que se describen en el documento anexo:

1. Política General de Seguridad y Privacidad de la Información, en cumplimiento del numeral 5.2 de la Norma ISO/IEC 27001:2013.
2. Política de Tratamiento y Protección de Datos Personales, en cumplimiento de los lineamientos de la Ley 1581 de 2012.
3. Política de Continuidad del Negocio o del Sistema de Gestión y Continuidad del Negocio, en cumplimiento de la Norma ISO/IEC 22301:2019, y el numeral A.17, Anexo A de la Norma ISO/IEC 27001:2013.
4. Política de recuperación ante desastres TIC.
5. Políticas específicas de seguridad y privacidad de la información.

Artículo 5. IMPLEMENTACIÓN. Todas las dependencias del Ministerio de Minas y Energía deberán implementar las políticas adoptadas a través del presente acto administrativo, conforme a sus responsabilidades y competencias.

Artículo 6. MODELO DE GOBERNANZA DE LA SEGURIDAD DIGITAL. Con el objeto de garantizar la adecuada gestión de la seguridad de la información en el Ministerio de Minas y Energía, se identifican los siguientes roles necesarios que interactuarán de manera articulada para la implementación, seguimiento y mejora del Modelo de Seguridad y Privacidad de la Información.

Artículo 7. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO. El Comité Institucional de Gestión y Desempeño del Ministerio de Minas y Energía es el encargado de asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.

Artículo 8. RESPONSABILIDADES DEL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO. Serán responsabilidades del Comité Institucional de Gestión y Desempeño del Ministerio de Minas y Energía en relación con el Modelo de Seguridad y Privacidad de la Información – MSPI, las siguientes:

1. Validar el alcance y las interfaces del Sistema General de Seguridad de la Información – SGSI-, al Sistema General de Continuidad del Negocio -SGCN- y el Modelo de Seguridad y Privacidad de la Información – MSPI- de acuerdo con el contexto y los intereses de las partes interesadas del Ministerio de Minas y Energía.
2. Validar y aprobar los objetivos de Seguridad de la Información.
3. Proponer acciones de alto nivel para apoyar el cumplimiento de los planes y proyectos de Seguridad de la Información.
4. Facilitar y promover el desarrollo de iniciativas sobre Seguridad de la Información.
5. Promover la importancia de cumplir los objetivos de Seguridad de la Información.
6. Validar la aplicación de la metodología corporativa de riesgos de Seguridad de la Información.
7. Validar el cumplimiento de los indicadores de Seguridad de la Información.

8. Asegurar que el personal con responsabilidades de Seguridad de la Información cuente con las competencias y conocimientos necesarios para el desempeño de sus funciones, esto será validado por la dependencia del Ministerio de Minas y Energía que, de conformidad con sus competencias, tenga la facultad de verificar el perfil y experiencia exigido para cada cargo.
9. Efectuar las revisiones regulares de la eficacia del Sistema General de Seguridad de la Información -SGSI-, basados en el resultado de las auditorías al Sistema General de Seguridad de la Información -SGSI-, los incidentes de Seguridad de la Información y la retroalimentación de las partes interesadas.

Artículo 9. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN Y/O QUIEN HAGA SUS VECES. Será el responsable por la gestión de Seguridad de la Información aplicando lo estipulado en el Sistema de Gestión de Seguridad de la Información -SGSI, reportando al nivel directivo asignado o en su defecto a las Mesas de Trabajo de las que trata la presente resolución, o al Comité Institucional de Gestión y Desempeño del Ministerio de Minas y Energía, sobre las políticas, objetivos y su cumplimiento.

Artículo 10. RESPONSABILIDADES DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN Y/O QUIEN HAGA SUS VECES. Como parte de las responsabilidades del Oficial de Seguridad de la Información se encuentran:

1. Orientar y brindar soporte a los líderes de los procesos para la gestión de activos de información, riesgos e incidentes de Seguridad de la Información, orientando a los líderes de los procesos para que cumplan con sus funciones de acuerdo con los roles y responsabilidades aplicables a su cargo.
2. Implementar, monitorear y mantener los componentes del Sistema General de Seguridad de la Información -SGSI- y del Sistema General de Continuidad del Negocio – SGCN-, según los parámetros definidos que corresponden al plan de Seguridad de la Información y que se basan en el análisis de contexto, las metodologías, políticas, procedimientos, estándares e indicadores de Seguridad de la Información.
3. Identificar oportunidades de mejora al Sistema General de Seguridad de la Información -SGSI- y al Sistema General de Continuidad del Negocio – SGCN- de acuerdo con los cambios en el Marco Legal y Regulatorio, la evolución de las amenazas sobre la información, los cambios en la organización o su entorno y gestionar su aplicación.
4. Analizar los requerimientos de Seguridad de la Información de los procesos, verificando que los controles y/o medidas implementadas se ajusten a las especificaciones definidas en los planes de tratamiento de riesgos.
5. Apoyar y asesorar técnicamente a las Mesas de Trabajo de las que trata la presente resolución o al Comité Institucional de Gestión y Desempeño del Ministerio de Minas y Energía en la aplicación de buenas prácticas de gestión relacionadas con Seguridad de la Información.
6. Coordinar con las Mesas de Trabajo de las que trata la presente resolución o al Comité Institucional de Gestión y Desempeño del Ministerio de Minas y Energía, las revisiones regulares para medir la eficacia del Sistema General de Seguridad de la Información -SGSI- y del Sistema General de Continuidad del Negocio – SGCN-.
7. Consolidar y presentar a las Mesas de Trabajo de las que trata la presente resolución o al Comité Institucional de Gestión y Desempeño del Ministerio de Minas y Energía, las necesidades o requerimientos de Seguridad de la Información.
8. Coordinar la medición de la eficacia de los controles de Seguridad de la Información implementados.
9. Definir, diligenciar y buscar el mejoramiento continuo de los indicadores de Seguridad de la Información establecidos en el Sistema General de Seguridad de la Información -SGSI- y del Sistema General de Continuidad del Negocio – SGCN.
10. Medir el nivel de cumplimiento de las políticas y estándares del Ministerio de Minas y Energía a través de los indicadores definidos para cada uno de los objetivos de la seguridad de la información en el Ministerio de Minas y Energía.
10. Reportar al Comité de Gestión y Desempeño los resultados de los indicadores de Seguridad de la Información, definiendo los planes requeridos junto con los responsables de los procesos para los ajustes o remediación necesarios.

11. Mantener contacto con autoridades y grupos de interés especializados en Seguridad de la Información preferiblemente especializados en el campo minero y energético a nivel mundial.
12. Gestionar y mantener actualizada la documentación establecida dentro del Sistema General de Seguridad de la Información -SGSI-.
13. Coordinar con el responsable del Sistema de Gestión el cumplimiento de los registros requeridos como evidencia, de conformidad con los requisitos del Sistema General de Seguridad de la Información -SGSI- y del Sistema General de Continuidad del Negocio – SGCN-.
14. Trabajar en conjunto con la Subdirección de Talento Humano para que se cumpla con el programa de capacitación y sensibilización en Seguridad de la Información.
15. Mantener actualizada la documentación del Sistema General de Seguridad de la Información -SGSI- y del Sistema General de Continuidad del Negocio – SGCN-con base en las necesidades del Ministerio.

Artículo 11. MESAS DE TRABAJO PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Para la implementación del Modelo de Seguridad y Privacidad de la Información, se implementarán las siguientes mesas de trabajo:

1. Mesa de Trabajo de Seguridad y Privacidad de la Información.
2. Mesa de Trabajo de Gestión de Continuidad del Negocio.

Estas mesas de trabajo se convocarán por el Oficial de Seguridad de la Información y/o quien haga sus veces.

Artículo 12. MESA DE TRABAJO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. La mesa de Trabajo de Seguridad y Privacidad de la información garantizará el apoyo y toma de decisiones al proceso de definición, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Modelo de Seguridad y Privacidad de la Información -MSPI- y el Sistema General de Seguridad de la Información -SGSI-.

Artículo 13. CONFORMACIÓN MESA DE TRABAJO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. La Mesa de Trabajo de Seguridad y Privacidad de la Información estará conformada por un representante de las siguientes áreas o dependencias del Ministerio de Minas y Energía:

1. Del Despacho de la Ministra y/o Ministro.
2. De la Secretaría General.
3. De la Oficina de Planeación y Gestión Internacional.
4. La Subdirección de Talento Humano.
5. La Oficina de Control Interno.
6. Del Grupo de Tecnologías de la Información y las Comunicaciones-TICS.
7. De la Subdirección Administrativa y Financiera.
8. Del Grupo de Relacionamiento con el Ciudadano y Gestión de la Información, y
9. El Oficial de Seguridad de la Información.

Artículo 14. FUNCIONES DE LA MESA DE TRABAJO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. La Mesa de Trabajo de Seguridad y Privacidad de la Información está liderada por el Oficial de Seguridad de la información y/o quien haga sus veces y tendrá las siguientes funciones:

1. Tomar decisiones que requiera el Modelo de Seguridad y Privacidad de la Información -MSPI- y el Sistema General de Seguridad de la Información -SGSI- y las propuestas que lleve el Oficial de Seguridad de la Información y/o quien haga sus veces, y cualquiera de sus miembros, respecto a los riesgos y a la seguridad de las informaciones requeridas para la Entidad.
2. Trabajar en forma articulada, activa y permanente con los líderes de procesos críticos en la ejecución y desarrollo de todas las actividades designadas para la implementación, sostenibilidad y mejora del Modelo de Seguridad y Privacidad de la Información -MSPI- de la Entidad.

3. Establecer, mantener y actualizar las políticas de Seguridad de la Información, la metodología para la gestión de riesgos, la metodología para la identificación y clasificación de los activos y la documentación propia del Sistema General de Seguridad de la Información -SGSI y del Modelo de Seguridad y Privacidad de la Información -MSPI-.
4. Monitorear el desarrollo y la implementación de las métricas de seguridad adecuadas para evaluar la efectividad y desempeño del Sistema General de Seguridad de la Información -SGSI y del Modelo de Seguridad y Privacidad de la Información MSPI.
5. Diseñar, sugerir o promover nuevas estrategias para la gestión de riesgos detectados.
6. Conocer y gestionar las alertas, amenazas y vulnerabilidades globales de Ciberseguridad y Seguridad y Privacidad de la Información, así como los planes de acción para el tratamiento de estas.
7. Mantener informado a todas las partes interesadas sobre la gestión macro del Modelo de Seguridad y Privacidad de la Información -MSPI- del Ministerio de Minas y Energía de manera periódica.

Artículo 15. MESA DE TRABAJO DE GESTIÓN DE CAMBIOS Y CONTINUIDAD DEL NEGOCIO. La Mesa de Trabajo de Gestión de Cambios y Continuidad del Negocio adoptará las decisiones relacionadas con la transición, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Análisis de Impacto del Negocio (BIA, por su sigla en inglés), el Sistema General de Continuidad del Negocio -SGCN- y el Sistema General de Seguridad de la Información -SGSI-.

Artículo 16. CONFORMACIÓN MESA DE TRABAJO DE GESTIÓN DE CAMBIOS Y CONTINUIDAD DEL NEGOCIO. La Mesa de Trabajo de Gestión de Cambios y Continuidad del Negocio estará conformada por un representante de las siguientes áreas o dependencias del Ministerio de Minas y Energía:

1. Del Despacho de la Ministra y/o Ministro.
2. De la Secretaría General.
3. De la Oficina de Planeación y Gestión Internacional.
4. La Subdirección de Talento Humano.
5. La Oficina de Control Interno.
6. Del Grupo de Tecnologías de la Información y las Comunicaciones-TICS.
7. De la Subdirección Administrativa y Financiera.
8. Del Grupo de Relacionamiento con el Ciudadano y Gestión de la Información, y
9. El Oficial de Seguridad de la Información.

Artículo 17. FUNCIONES MESA DE TRABAJO DE GESTIÓN DE CAMBIOS Y CONTINUIDAD DEL NEGOCIO. La Mesa de Trabajo de Gestión de Cambios y Continuidad del Negocio está liderada por el Oficial de Continuidad del Negocio y/o quien haga sus veces, y tendrá las siguientes funciones:

1. Tomar decisiones que requiera el Sistema General de Continuidad del Negocio -SGCN- y las propuestas que lleve el Oficial de Continuidad del Negocio y/o quien haga sus veces, y cualquiera de sus miembros, respecto a los riesgos y temas de Continuidad del Negocio requeridos para la Entidad.
2. Trabajar en forma articulada, activa y permanente con los líderes de procesos críticos en la ejecución y desarrollo de todas las actividades designadas para la implementación, sostenibilidad y mejora del Sistema de Gestión de Continuidad del Negocio -SGCN- de la Entidad.
3. Establecer, mantener y actualizar las políticas de Continuidad del Negocio, la metodología para la gestión de riesgos y la documentación propia del Sistema de Gestión de Continuidad del Negocio -SGCN-.
4. Desarrollar y liderar la implementación de métricas de Continuidad del Negocio adecuadas para evaluar la efectividad y desempeño del Sistema de Gestión de Continuidad del Negocio -SGCN-.
5. Diseñar, sugerir o promover nuevas estrategias para la gestión de riesgos detectados.
6. Conocer y gestionar las alertas, amenazas y vulnerabilidades globales de Continuidad del Negocio, así como los planes de acción para el tratamiento de estas.

7. Mantener informadas a todas las partes interesadas sobre la gestión macro del Sistema de Gestión de Continuidad del Negocio -SGCN- de la Entidad de manera periódica.
8. Velar por que los programas de concientización en Continuidad del Negocio se lleven a cabo según lo planeado.
9. Asegurar que la adaptación al cambio de los usuarios de base, versus usuarios críticos preparados y formados para atender un plan de contingencias, estén apoyados en planes de sensibilización, capacitación, compromiso y sentido de pertenencia del rol a asumir ante la materialización de un evento o hecho inesperado.

Artículo 18. DECISIÓN. Las decisiones y temas relacionados con la *"Política de Seguridad y Privacidad de la Información"* serán discutidos en el Comité Institucional de Gestión y Desempeño del Ministerio de Minas y Energía, cuando así se determine, con el apoyo del Oficial de Seguridad de la entidad y/o quien haga sus veces, y siguiendo los lineamientos que en esta materia existan en la administración pública colombiana.

Artículo 19. ACTUALIZACIÓN. La Política de Seguridad y Privacidad de la Información y conexas al Modelo de la Seguridad y Privacidad de la Información -MSPI- serán revisadas y actualizadas de acuerdo con las necesidades o cambios en la estrategia institucional, las buenas prácticas y/o los lineamientos gubernamentales.

Artículo 20. COMUNICACIÓN. Comunicar las Políticas de las que trata la presente resolución a todos los colaboradores del Ministerio de Minas y Energía mediante su publicación en la página web de la entidad.

Artículo 21. VIGENCIA Y DEROGATORIA. La presente Resolución rige a partir de la fecha de su publicación, y deroga la Resolución 4 0362 del 3 de mayo de 2017.

PUBLÍQUESE Y CÚMPLASE
Dada en Bogotá, D. C., a los 01 NOV 2023

OMAR ANDRÉS CAMACHO MORALES
Ministro de Minas y Energía

Proyectó: Oscar Sánchez S. / Carlos Javier Osorio B.
Revisó: Juan José Cedeño López / Jorge Eduardo Salgado Ardila / Jorge Eliecer Lozano Ospina / Feiber Alexander Ochoa
Aprobó: Nelson Javier Vásquez Torres

POLÍTICAS APLICABLES AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI DEL MINISTERIO DE MINAS Y ENERGÍA.

Política General de la Seguridad y Privacidad de la Información, Política de Tratamiento y Protección de Datos Personales, Política de Continuidad del Negocio o del Sistema de Gestión y Continuidad del Negocio, Política de Recuperación ante Desastres TIC y Políticas Específicas de Seguridad y Privacidad de la Información en el Ministerio de Minas y Energía.

El presente anexo técnico contiene los principios aplicables al Modelo de Seguridad y Privacidad de la Información del Ministerio de Minas y Energía y la definición de las políticas aplicables a este modelo en el marco de la normatividad vigente como son:

1. Política General de Seguridad y Privacidad de la Información.
2. Política de Tratamiento y Protección de Datos Personales.
3. Política de Continuidad del Negocio o del Sistema de Gestión y Continuidad del Negocio.
4. Política de Recuperación ante Desastres TIC.
5. Políticas específicas de seguridad y privacidad de la información.

1. POLÍTICAS.

1.1. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La Política General de Seguridad y Privacidad de la Información integra los lineamientos que representan la posición de la Dirección del MINENERGÍA, con respecto a la protección de la información y los datos que se procesan, transportan o transmiten y se almacenan en los activos de información de la entidad.

Estos activos están integrados por: usuarios, la información y los datos, los procesos y las tecnologías de información y comunicación, incluido el hardware y el software, que en su conjunto, soportan los procesos de la entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información -SGSI.

Frente a estos activos, se establecen los riesgos que puedan comprometer su confidencialidad, integridad o disponibilidad y estos riesgos se gestionan, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad y privacidad de la información.

El detalle y las guías para la implementación de esta política se encuentran establecidas en el Manual de Políticas del Sistema de Gestión de Seguridad de la Información – MPSGSI de la entidad.

El MINENERGÍA, establece la compatibilidad de esta política de seguridad de la información con los objetivos de seguridad de la información, establecidos en el Manual del Sistema General de Seguridad de la Información.

A continuación, se establece el decálogo de seguridad que soporta el establecimiento de las políticas específicas, el Modelo de Seguridad y Privacidad de la Información - MSPI y el Sistema de Gestión de Seguridad de la Información - SGSI del MINENERGÍA:

1. El MINENERGÍA gestionará las medidas necesarias y pertinentes para definir, implementar, operar y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información (SGSI), soportado en lineamientos claros alineados a las necesidades de la Entidad y a los requerimientos regulatorios que le aplican a su naturaleza.

2. Las responsabilidades frente a la seguridad y privacidad de la información, descritas en el numeral 1.5 *"Políticas específicas de seguridad y privacidad de la información"* del presente documento, deberán ser compartidas, publicadas y aceptadas por cada uno de los usuarios.

3. El MINENERGÍA protegerá la información generada, procesada o resguardada por los procesos críticos de negocio y los activos de información que hacen parte de estos.

4. El MINENERGÍA protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales, debido a un uso incorrecto de esta o de amenazas originadas por parte del personal. Para ello, es fundamental la aplicación de controles, de acuerdo con la clasificación de la información de su propiedad o en custodia.

5. El MINENERGÍA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos y controlará la operación de sus procesos críticos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

6. El MINENERGÍA implementará control de acceso a la información, sistemas y recursos de red.

7. El MINENERGÍA integrará la seguridad de la información como parte del ciclo de vida de los sistemas de información.

8. El MINENERGÍA, a través de una adecuada gestión de los eventos o incidentes de seguridad y las vulnerabilidades asociadas con los sistemas de información, mejorará de manera efectiva su modelo de seguridad.

9. El MINENERGÍA establecerá la disponibilidad de sus procesos críticos de negocio, y la continuidad de su operación, basado en el impacto que pueden generar los eventos o desastres, sobre la operación y los activos críticos de la Entidad.

10. El MINENERGÍA definirá y hará seguimiento sobre el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

1.1.1. Alcance/Aplicabilidad.

Esta política aplica a los servidores públicos, contratistas, proveedores y/o terceros usuarios cuando se recolecte, procese, almacene, recupere, intercambie, consulte información y demás, en el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

1.1.2. Nivel de Cumplimiento de la Política.

Todas las personas cubiertas por el alcance y aplicabilidad deben dar cumplimiento a la presente política.

1.1.3. Excepciones a la política.

Cualquier excepción a la presente política deberá ser escalada por el Oficial de Seguridad de la Información ante la Mesa de Trabajo de Seguridad y Privacidad de la Información.

1.1.4. Revisiones.

Esta política será revisada por el Oficial de Seguridad de la Información sobre su aplicación y pertinencia de manera anual o cuando ocurra un cambio significativo en alguno de los componentes del Sistema de Gestión de Seguridad de la Información -SGSI, en las partes interesadas o en cambios significativos internos de la Entidad.

1.2. POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES.

La presente Política de Tratamiento y Protección de Datos Personales es elaborada de conformidad con lo dispuesto en los artículos 15 y 20 de la Constitución Política de Colombia, la Ley Estatutaria 1581 de 2012, el Decreto Reglamentario 1377 de 2013, compilado en el Decreto 1074 de 2015, Único Reglamentario del Sector Comercio, Industria y Turismo y demás disposiciones complementarias y será aplicada por MINENERGÍA, respecto de la recolección, almacenamiento, uso, circulación, supresión y de todas aquellas actividades que constituyan tratamiento de datos personales.

Principios para el establecimiento de la Política de Tratamiento y Protección de Datos Personales a cumplir por el MINENERGÍA:

1. Principio de la Legalidad: El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.

2. Principio de finalidad: Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.

3. Principio de libertad: El tratamiento solo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.

4. Principio de veracidad o calidad: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.

5. Principio de transparencia: Garantizar al titular de los datos, el derecho a obtener información que le concierna del encargado del tratamiento.

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.

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.
8. Principio de confidencialidad: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva y confidencialidad de dicha información.

1.2.1. Alcance/Aplicabilidad.

Esta política aplica a los servidores públicos, contratistas, proveedores y/o terceros usuarios.

1.2.2. Nivel de Cumplimiento de la Política.

Todas las personas cubiertas por el alcance y aplicabilidad deben dar cumplimiento a la presente política.

1.2.3. Excepciones a la política.

Cualquier modificación a la presente política, debe ser escalada al Oficial de Seguridad de la Información y será revisada por la Mesa de Trabajo de Seguridad y Privacidad de la información.

1.2.4. Revisiones.

Esta política será revisada por el Oficial de Seguridad de la Información sobre su aplicación y pertinencia de manera anual o cuando ocurra un cambio significativo en alguno de los componentes del SGSI, el MSPI, en las partes interesadas o en cambios significativos internos de la Entidad.

1.3. POLÍTICA DE CONTINUIDAD DEL NEGOCIO O DEL SISTEMA DE GESTIÓN Y CONTINUIDAD DEL NEGOCIO (SGCN).

El MINENERGÍA, en su compromiso con su misión de formular y adoptar políticas dirigidas al aprovechamiento sostenible de los recursos mineros y energéticos, para contribuir al desarrollo económico y social del país, realiza los preparativos necesarios, y planifica los procedimientos necesarios para dar la respuesta adecuada ante un incidente o evento que ponga en riesgo la continuidad del negocio, desde el instante en el que se declare el desastre o contingencia hasta el regreso a la normalidad.

Con este compromiso, el MINENERGÍA establece un Sistema de Gestión de Continuidad del Negocio -SGCN, que brinda la resiliencia necesaria para continuar brindando sus funciones críticas de negocio y cumpliendo con sus obligaciones legales y contractuales.

El Ministerio de Minas y Energía se asegurará de establecer los objetivos de continuidad del negocio y de comunicarlos a los procesos críticos y a todos los interesados de acuerdo con sus competencias.

Para esto establecerá el plan de implementación que permitirá alcanzar los objetivos de continuidad del negocio.

Principios para la planeación, implementación, validación y mejora del Sistema General de Continuidad del Negocio -SGCN:

1. Sostener las operaciones del Ministerio y sus servicios críticos en un nivel de servicio aceptable que permita cumplir con sus obligaciones legales y contractuales.
2. Minimizar la exposición del Ministerio a sanciones legales por incumplimiento con las partes interesadas.
3. Mitigar los efectos negativos que puedan producirse en los planes estratégicos del Ministerio.
4. Mantener la reputación e imagen del Ministerio.

1.3.1. Alcance/Aplicabilidad.

Esta política aplica a los servidores públicos, contratistas, proveedores y/o terceros usuarios.

1.3.2. Nivel de Cumplimiento de la Política.

Todas las personas cubiertas por el alcance y aplicabilidad deben dar cumplimiento a la presente política.

1.3.3. Excepciones a la política.

Cualquier modificación a la presente política, debe ser escalada al Oficial de seguridad de la información y será revisada por la Mesa de Trabajo de Cambios y Continuidad de Negocio.

1.3.4. Revisiones.

Esta política será revisada por el Oficial de Seguridad de la Información sobre su aplicación y pertinencia de manera anual o cuando ocurra un cambio significativo en alguno de los componentes del Sistema General de Seguridad de la Información - SGSI, el Modelo de Seguridad y Privacidad de la Información - MSPI, en las partes interesadas o en cambios significativos internos de la Entidad.

1.4. POLÍTICA DE RECUPERACIÓN ANTE DESASTRES TIC.

El MINENERGÍA dedicará los esfuerzos necesarios y suficientes para reducir la probabilidad de interrupciones del negocio. En el caso que se produjera una interrupción, asegurar que la misma no exceda los objetivos de tiempo de recuperación y garantizar la disponibilidad de todos los recursos necesarios para la recuperación.

La Gestión de la Continuidad de la Operación de TIC se implementa para la Gestión de Tecnología de Información y Comunicación del MINENERGÍA, con especial atención sobre las actividades identificadas como críticas durante el análisis de impacto en el negocio.

1.4.1. Alcance/Aplicabilidad.

Esta política aplica a los servidores públicos, contratistas, proveedores y/o terceros usuarios.

1.4.2. Nivel de Cumplimiento de la Política.

Todas las personas cubiertas por el alcance y aplicabilidad deben dar cumplimiento a la presente política.

1.4.3. Excepciones a la política.

Cualquier modificación a la presente política, debe ser escalada al Oficial de seguridad de la información y será revisada por la mesa de trabajo de cambios y continuidad de negocio.

1.4.4. Revisiones.

Esta política será revisada sobre su aplicación y pertinencia de manera anual o cuando ocurra un cambio significativo en alguno de los componentes del Sistema General de Seguridad de la Información - SGSI, el Modelo de Seguridad y Privacidad de la Información - MSPI, en las partes interesadas o en cambios significativos internos de la Entidad.

1.5. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

A continuación, se relacionan las políticas que van enfocadas en la seguridad y privacidad de la información:

1.5.1 POLÍTICA DE GESTIÓN DE ACTIVOS.

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

Los activos de información gestionados en todos los procesos del MINENERGÍA, deben cumplir con lo siguiente:

Seguir las políticas y procedimientos establecidos para la identificación y clasificación de activos, usos aceptables y entrega y devolución de activos.

1.5.2. POLÍTICA USO ACEPTABLE DE ACTIVOS.

Las partes interesadas, son responsables de un adecuado y racional uso de los activos de información que se usan en los procesos del MINENERGÍA. Es decir, no se pueden usar para propósitos ni con configuraciones diferentes para los cuales fueron definidos por el MINENERGÍA.

1.5.3. POLÍTICA USO CORREO ELECTRÓNICO.

Toda comunicación por correo electrónico entre las partes interesadas debe efectuarse mediante el uso del sistema aprobado por MINENERGÍA (correo institucional). Toda información transmitida por este medio es considerada como propiedad de la Entidad.

Las partes interesadas, no podrán enviar correos internos o externos, que puedan perjudicar la imagen de la Entidad. Así mismo, estos son responsables del contenido de las comunicaciones enviadas, por lo cual se debe revisar y validar la información a enviar a través del correo electrónico institucional.

El MINENERGÍA se reserva el derecho a monitorear, auditar y vigilar los correos electrónicos institucionales para garantizar que sea utilizado solo para propósitos laborales, mediante una herramienta controlada en su uso por el Oficial de Seguridad de la Información, sin que tenga acceso al contenido de estos.

1.5.4. POLÍTICA USO DE INTERNET.

La utilización del servicio de internet ofrecido por el MINENERGÍA debe estar limitado únicamente a asuntos laborales y de fortalecimiento de competencias. El uso inadecuado o abuso del servicio de Internet por las partes interesadas, dará lugar a procesos de investigación y sanciones disciplinarias.

La navegación en Internet debe realizarse de forma razonable y con propósitos laborales o de fortalecimiento de competencias.

El uso de redes sociales dentro de la Entidad solamente está habilitado a los usuarios autorizados que, por necesidades específicas de sus funciones así lo requieran, con la autorización previa, visto bueno del Jefe de la dependencia, y solicitud hecha a la Coordinación del Grupo TICS para aprobación, teniendo en cuenta que, de no ser así, se pueden generar problemas de inseguridad.

La Entidad debe garantizar que las dependencias responsables de publicar información institucional a través de estos medios, lo puedan hacer adecuadamente y pueden asesorarse con el Oficial de Seguridad de la Información previamente.

Cada parte interesada, es responsable de asegurar que el uso de redes externas no comprometa los activos de información de la Entidad, teniendo en cuenta que son fuentes usadas para hurto de información y de explotación de vulnerabilidades de seguridad.

Está prohibido el ingreso a páginas que atenten contra la moral y las buenas costumbres de la Entidad. No se permite la navegación a sitios con contenidos contrarios a la ley o que representen peligro para el MINENERGÍA como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por el Oficial de Seguridad de la Información y aprobado por una mesa de trabajo del Plan de Desarrollo Administrativo (PDA).

En el evento de requerirse descargar programas, se deberá elevar solicitud desde la dependencia del Ministerio, dirigida a la Coordinación del Grupo TICS, indicando las razones, motivos, pertinencia funcional y tiempo de uso del software, con el objeto de poder contar con la autorización respectiva

1.5.5. POLÍTICA CLASIFICACIÓN DE LA INFORMACIÓN.

Toda información que se gestione en la Entidad de acuerdo con su criticidad, sensibilidad y reserva, teniendo en cuenta las leyes y normatividad vigentes que afecten a la Entidad, se deberá generar por un procedimiento de clasificación de la información, para que los propietarios de esta la cataloguen según los niveles definidos sin excepción.

Los líderes de cada proceso deben velar porque se realice la clasificación de la información manejada en su proceso, así como de revisar anualmente la clasificación de los activos involucrados en el proceso, y de ser necesario realizar las actualizaciones requeridas.

El Comité de Seguridad y Privacidad de la Información, debe realizar la gestión para socializar y divulgar el procedimiento a todas las partes interesadas de la Entidad, para su estricto cumplimiento.

En cumplimiento de la Ley 1712 de 2014, la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y según las definiciones del artículo 6, se deben manejar los siguientes tres (3) niveles de clasificación:

1. Información pública

Esta información es creada en desarrollo de la misión de la Entidad, la cual puede ser publicada para dar cumplimiento a la normatividad aplicable o política de divulgación de la Entidad. La información está disponible para las partes interesadas y la ciudadanía en general.

Ejemplos de este tipo de información: plan de Auditoría Independiente, Plan de Adquisiciones, Requerimiento de Información de la Procuraduría, rendición de cuentas sobre la gestión de la Entidad, indicadores financieros, procesos y procedimientos de atención a la ciudadanía.

2. Información pública clasificada

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las

circunstancias legítimas y necesarias, y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014, corregido por el artículo 2 del Decreto 1494 de 2015.

Ejemplos de este tipo de información: liquidación de nómina de funcionarios, informes gestión de combustible, peticiones quejas y reclamos presentadas por los usuarios, secretos comerciales, industriales y profesionales.

3. Información pública reservada

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso por daño de intereses públicos consagrados en el artículo 19 de la Ley 1712 de 2014.

Ejemplo de este tipo de información: investigaciones de procesos disciplinarios, planos de exploración de pozos petroleros y minas, puntos de ubicación de almacenamiento y distribución de combustible, diagnósticos y recomendaciones de las partes interesadas.

1.5.6. POLÍTICA DISPOSITIVOS MÓVILES.

El MINENERGÍA controla, gestiona y aprueba el manejo de los dispositivos móviles (teléfonos inteligentes, portátiles, discos duros, USB, DVD, entre otros) institucionales y personales que hagan uso de los sistema de información y/o equipos de la Entidad, previa aprobación del Oficial de Seguridad de la Información, y velará por el uso adecuado y seguro de los mismos, para que este control sea implementado y que requiera la aprobación por la Mesa de Trabajo de Seguridad y Privacidad de la Información.

El acceso físico a las instalaciones del MINENERGÍA, de los dispositivos personales como portátiles, tabletas, notebook, entre otros, de propiedad de las partes interesadas, serán controlados, registrados y aprobados previamente para su uso en la red de la Entidad por parte de los Grupos de Gestión de Recursos Físicos y el Grupo TIC, validados por el Oficial de Seguridad de la información o quien haga sus veces, sin excepción.

1.5.7. POLÍTICA PANTALLA Y ESCRITORIO LIMPIO.

El MINENERGÍA establece las pautas para preservar la información, por medio de buenas prácticas en el manejo de documentos físicos y lógicos, medios de almacenamiento removibles y pantallas de los dispositivos de procesamiento de información durante y fuera de la jornada laboral.

Las partes interesadas procurarán conservar el escritorio libre de documentos o dispositivos de almacenamiento, con el fin de evitar acceso no autorizado, pérdida y daño de la información de la Entidad.

La información confidencial, ubicada en medios físicos o impresos debe ser guardada bajo llave, cuando no está siendo utilizada, especialmente cuando la oficina se encuentre vacía.

Las partes interesadas deben bloquear la pantalla de su computador con el protector de pantalla, cuando no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

Los documentos que contienen información confidencial deberán ser retirados inmediatamente de la impresora, fotocopiadora o fax, por las partes interesadas responsables, no se deben dejar sin custodia o abandonadas, si esto sucede será tratado como un incidente de seguridad de la información.

1.5.8. POLÍTICA CONTROL DE ACCESO.

El Oficial de Seguridad de la Información debe validar todo acceso a nivel de red, instalaciones físicas, sistemas operativos, bases de datos y aplicaciones. Los controles deben estar soportados por una cultura de riesgos y seguridad, así mismo, limitar el acceso a la información de la Entidad al mínimo requerido (principio del mínimo privilegio), para la realización de los roles o funciones.

Además, se requiere permitir identificar de manera inequívoca cada parte interesada, y hacer un seguimiento periódico o aleatorio de las actividades que estos realizan para la Entidad.

Todos los usuarios deberán asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.

1.5.9. POLÍTICA GESTIÓN DE CONTRASEÑAS

Para controlar el acceso de la información y restringirla solo al personal autorizado conforme el perfil de acceso, el Oficial de Seguridad de la Información, definirá los lineamientos para la administración adecuada de contraseñas para la Entidad.

Siendo las contraseñas un medio de validación de la identidad digital de un usuario (partes interesadas) y por ende un medio para establecer derechos de acceso a los sistemas de información, el MINENERGÍA garantiza la ejecución de actividades que promuevan la conciencia e implementación de mecanismos que permitan controlar que los usuarios siguen buenas prácticas de seguridad en la selección, uso y protección de contraseñas.

Las partes interesadas son responsables del uso de las contraseñas de acceso que se le asignen para la utilización de los sistemas de información de la Entidad, cualquier anomalía al respecto será tratada como incidente de Seguridad de la Información.

1.5.10. POLÍTICA GESTIÓN DE RIESGOS.

Se adopta para el Sistema de Gestión de Seguridad de la Información - SGSI, la guía para la administración del riesgo elaborado por el Departamento Administrativo de la Función Pública – DAFP, para la gestión de riesgos integral para el MINENERGÍA, que así misma está basada en la ISO 31000 para la Gestión del Riesgo. A nivel interno se adoptará el Procedimiento Administración del Riesgo de la Entidad.

Los riesgos de Seguridad de la Información identificados en el MINENERGÍA, deben tener un tratamiento adecuado que permita minimizarlos. Se debe realizar seguimiento de manera trimestral por el líder o dueño del proceso, para asegurar su correcta gestión y tratamiento.

Los riesgos de Seguridad de la Información deben ser incluidos en todas las matrices de riesgos de todos los procesos del MINENERGÍA.

Los riesgos de Seguridad de la Información deben ser tratados por la Mesa de Trabajo de Seguridad y Privacidad de la Información y evidenciar por medio de registros el seguimiento de estos, por lo menos dos (2) veces al año.

Toda adquisición de nueva tecnología o soluciones de Seguridad Informática, debe basarse en los resultados de los riesgos de Seguridad de la Información realizados en el MINENERGÍA previamente, para que tengan una base que sustente las inversiones y los beneficios o el tratamiento al riesgo establecido.

1.5.11. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD.

El MINENERGÍA incentivará a que todas las partes interesadas que gestionen activos de información reporten incidentes de seguridad o cualquier evento que pueda afectar los criterios de confidencialidad, integridad, disponibilidad y privacidad de la información o aquellos aspectos que sean sospechosos o derivados del mal uso de estos en la Entidad.

En la Entidad se asignan como responsables para la gestión de los incidentes de seguridad, al Oficial de Seguridad de la Información y a la Mesa de Trabajo de Seguridad y Privacidad de la Información para la toma de decisiones, quienes deben asegurar que se realiza una adecuada evaluación del impacto de los incidentes de seguridad presentados y que sean relevantes, así como definir los procedimientos de preparación, detección y análisis, contención/respuesta, erradicación y recuperación del manejo dado al incidente, para el restablecimiento de la plataforma y/o servicio afectado.

1.5.12. POLÍTICA GESTIÓN DEL CAMBIO.

El MINENERGÍA vela por que cualquier cambio a los equipos o sistemas de información, se realicen de manera gestionada y controlada, evaluando los riesgos previamente, y acorde a las necesidades y requerimientos de la Entidad, bajo la metodología de ISO 20000 o ITIL.

Todo requerimiento de creación, mejora o reporte, que genere un cambio en los sistemas de información de la Entidad, debe ser solicitado o notificado formalmente al Grupo TIC previamente para su validación, y se aprobará por el dueño del proceso afectado por el cambio.

El MINENERGÍA conforma una Mesa de Trabajo de Cambios y Continuidad del Negocio, para que el Oficial de Seguridad de la Información y junto con el Grupo TIC, evalúen y autoricen la instalación, cambio o eliminación de componentes de la plataforma tecnológica y de los sistemas de información de la Entidad.

El Grupo TIC, 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.

Los responsables de los cambios, deben informar antes de la implementación de un cambio, a las dependencias o partes interesadas que puedan verse afectadas, con el fin de evitar falta de operatividad.

Todo cambio realizado a un recurso informático y/o sistemas de información, debe quedar formalmente documentado, desde la solicitud hasta su evaluación, lo cual proveerá un mecanismo de trazabilidad y seguimiento al cumplimiento de los procedimientos establecidos.

1.5.13. POLÍTICA RESPALDO Y COPIAS DE SEGURIDAD.

El MINENERGÍA genera continuamente copias de respaldo y almacenamiento seguro de la información crítica, proporcionando los recursos para medios de respaldo adecuados y estableciendo los procedimientos y mecanismos para la realización de estas actividades de manera efectiva, con el fin de asegurar que toda la información esencial de la Entidad pueda ser restaurada en caso de ser necesario.

El almacenamiento de la información de la Entidad se debe realizar de manera interna y externa, de acuerdo con su clasificación y con previa validación del Oficial de Seguridad de la Información.

Las copias de respaldos se deben almacenar en un sitio lejano con protección física, lógica y ambiental, a una distancia suficiente para escapar a cualquier daño causado por desastres. El sitio externo donde se resguarden las copias de respaldo, debe contar con los controles de seguridad física y medioambiental apropiados, y en lo posible estar certificados en la gestión de seguridad de la información.

Se recomienda usar otra locación externa o ver la viabilidad de uso de empresas en el mercado que se dedican a esto de manera segura y confiable.

Se definen procedimientos de restauración para los medios de respaldo, se verificarán y probarán trimestralmente, para garantizar la disponibilidad de la información en caso de contingencia o desastre, y se deben reportar los resultados al Oficial de Seguridad de la Información y a la Oficina de Control Interno.

1.5.14. POLÍTICAS DE ELIMINACIÓN Y DESTRUCCIÓN SEGURA DE INFORMACIÓN.

El MINENERGÍA establece los lineamientos para que la eliminación, destrucción o borrado seguro de la información, se realice de forma adecuada en el activo de información que la contenga. La eliminación segura de información es un mecanismo de control para prevenir la divulgación de información confidencial de la Entidad.

El Oficial de Seguridad de la Información, con apoyo de la Oficina de Control Interno, puede validar y revisar de manera semestral, la ejecución correcta del procedimiento realizado por el proveedor de alistamiento de equipos.

1.5.15. POLÍTICA TRANSFERENCIA DE INFORMACIÓN Y CIFRADO

El MINENERGÍA, asegura la protección de la información, en el momento de ser transferida o intercambiada interna y externamente con cualquier otra organización, por lo cual establece procedimientos y controles mínimos requeridos para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información.

La Entidad define modelos de acuerdos de confidencialidad y/o de intercambio de información con los proveedores (terceras partes), que incluyan los compromisos adquiridos y penalidades por el incumplimiento de dichos acuerdos. Entre los aspectos más importantes se consideran los siguientes:

- **a.** Responsabilidades y procedimientos para controlar la transmisión y recepción de información.
- **b.** Procedimientos para garantizar la trazabilidad y no repudio.
- **c.** Responsabilidades en caso de incidentes de seguridad de la información.
- **d.** Políticas, procedimientos y normas para proteger la información y los medios contenedores.
- **e.** Prohibición de divulgar la información entregada.
- **f.** Destrucción segura de la información una vez cumpla el objeto del contrato.

La Mesa de Trabajo de Seguridad y Privacidad de la Información y el Oficial de Seguridad de la Información, definen y establecen procedimientos de intercambio de información segura, con las diferentes partes interesadas, que forman parte de la operación de la Entidad, teniendo en cuenta la utilización de medios de transmisión confiables y la adopción de controles y herramientas seguras, con el fin de proteger la confidencialidad e integridad de la información.

1.5.16. POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

Se utilizarán controles criptográficos implementados por el área de TIC y el Oficial de Seguridad de la Información, en los siguientes casos:

- **a.** Para la protección de claves de acceso a sistemas, datos y servicios o entornos de trabajo.
- **b.** Para la transmisión de información clasificada, fuera del ámbito de la Entidad a través de redes públicas, como el correo electrónico.
- **c.** Para la protección de información, cuando así surja de la evaluación de riesgos realizada.
- **d.** Para proteger información confidencial en medios removibles o en copias de respaldo.
- **e.** Se desarrollan procedimientos respecto de la administración de llaves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las llaves y en cuanto al reemplazo de las claves de cifrado.
- **f.** En activos en los que sea necesario el control de software malicioso y se les haya aplicado criptografía, el área de seguridad de la información y de TIC, implementarán un procedimiento para descifrar la información o los archivos para permitir el escaneo y que luego pueda volver a ser cifrada.
- **g.** Por solicitud o requerimiento directo de partes interesadas sobre algún desarrollo o información específica.

1.5.17. POLÍTICA GESTIÓN DE LLAVES

Se establece la gestión de llaves para apoyar el uso de técnicas criptográficas en la Entidad.

Se define el uso, protección y tiempo de vida de las llaves criptográficas, requisitos para la gestión de llaves criptográficas durante todo su ciclo de vida, incluida la generación, almacenamiento, archivo, recuperación, distribución, retiro y destrucción de las llaves.

Todas las llaves criptográficas deben tener protección contra modificación, pérdida o destrucción.

El equipo usado para generar, almacenar y archivar las claves está protegido por medios físicos.

Un sistema de gestión de llaves debe basar en un conjunto acordado de normas, procedimientos y métodos seguros para:

- **a.** Generar llaves para diferentes sistemas criptográficos y diferentes aplicaciones.
- **b.** Generar y obtener certificados de llaves públicas.
- **c.** Distribuir llaves a las entidades previstas, incluyendo la forma de recibir y activar las llaves.
- **d.** Almacenar las llaves, incluyendo la forma en que los usuarios autorizados obtienen acceso a ellas.
- **e.** Cambiar o actualizar las llaves, incluyendo las reglas sobre cuándo se deberían cambiar y cómo hacerlo.
- **f.** Dar tratamiento a las llaves cuya seguridad está comprometida.
- **g.** Revocar las llaves, incluyendo la forma de retirarlas o desactivarlas, por ejemplo, cuando la seguridad de las llaves ha estado comprometida, o cuando un usuario deja la Entidad (en cuyo caso las llaves también se deberían archivar).
- **h.** Recuperar las llaves que estén pérdidas o dañadas.
- **i.** Hacer copias de respaldo de las llaves o archivarlas.
- **j.** Destruir las llaves.
- **k.** Registrar y auditar las actividades relacionadas con gestión de llaves.

1.5.18. POLÍTICA SEGURIDAD FÍSICA Y ÁREAS SEGURAS

El MINENERGÍA provee, implementa y realiza seguimiento a los mecanismos de seguridad física y control de acceso, que aseguren las zonas y perímetros de sus instalaciones físicas y aquellos que le permiten controlar y gestionar los riesgos frente a las amenazas físicas, externas e internas y las condiciones medioambientales de los espacios físicos de la Entidad.

Las áreas físicas destinadas para el procesamiento o almacenamiento de información pública clasificada o reservada, así como aquellas en las que se encuentren los equipos y sistemas de información y comunicaciones, se consideran áreas o zonas seguras.

Los ingresos y egresos de todos los usuarios a las instalaciones físicas del MINENERGÍA, deben ser registrados sin excepción, es decir, que las partes interesadas, deben cumplir completamente con los controles físicos implantados en la Entidad.

Las solicitudes de acceso a las áreas seguras deben ser aprobadas por el responsable del área física e informar al Oficial de Seguridad de la Información para todas las partes interesadas y visitantes. Adicionalmente, siempre debe estar acompañado de un funcionario de dicha dependencia durante toda la visita.

La protección física, se llevará a cabo mediante la creación de diversas barreras o medidas de control, alrededor de las dependencias donde se encuentran instalados los dispositivos de procesamiento y almacenamiento de la información de la Entidad.

El MINENERGÍA define los perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado y cualquier otra condición crítica para el correcto funcionamiento de los equipos y sistemas de información.

En la selección de los mecanismos de protección de un área segura, se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión y otras formas de desastres naturales o provocados.

De igual manera, se tomarán en cuenta las disposiciones y normatividad asociada a la seguridad física, y se considerarán las amenazas a la seguridad que representan los edificios y zonas cercanas.

Se deben realizar estudios externos de seguridad física por entes especializados, de manera anual y en acompañamiento del Oficial de Seguridad de la información.

La información sobre la naturaleza, localización y disposición de los sistemas de procesamiento y almacenamiento de información del MINENERGÍA, es de carácter clasificado y reservado, solo debe ser divulgado a quienes demuestren la necesidad de conocer, y sean autorizados por el responsable del área segura, y validado por el Oficial de Seguridad de la Información.

Está prohibido el ingreso de equipos de grabación de video y/o audio, fotografía o dispositivos móviles inteligentes, que incluyan esas aplicaciones, sin autorización previa del responsable del área segura y validado por el Oficial de Seguridad de la Información.

Las zonas o áreas seguras deben estar demarcadas y con el aviso de acceso restringido.

1.5.19. POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

1.5.19.1. Adquisición y mantenimiento de sistemas.

El MINENERGÍA, debe asegurar que la Seguridad de la Información sea una parte integral de los sistemas de información durante todo el ciclo de vida, incluyendo los requisitos para sistemas de información que prestan servicios sobre redes públicas.

1.5.19.2. Análisis y especificación de requisitos de seguridad.

El MINENERGÍA establecerá los requisitos relacionados con Seguridad de la Información, los cuales deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

1.5.19.3. Seguridad de servicios de las aplicaciones en redes públicas.

El Proceso de gestión de tecnología de información y comunicación de la Entidad, debe proteger de actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizada de la información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas. Para esto cuando se trate de aplicaciones que se vayan a usar en entornos web, se deberán seguir ciclos de mejores prácticas de codificación segura, que incluyan análisis de riesgos y gestión de vulnerabilidades web.

1.5.19.4. Protección de transacciones de los servicios de las aplicaciones.

La información involucrada en las transacciones de los servicios de las aplicaciones, se debe proteger para evitar la trasmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizados, por medio de controles que establecerá el Proceso de gestión de tecnología de información y comunicación del Ministerio.

1.5.19.5. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.

Cuando se cambian las plataformas de operación, el proceso de gestión de tecnología de información y comunicación, debe revisar las aplicaciones críticas del Ministerio, y someterlas a prueba, para asegurar que no haya impacto adverso en las operaciones o seguridad de la Entidad, provocado por los cambios.

1.5.19.6. Restricciones en los cambios a los paquetes de software.

Los cambios a los paquetes de software son autorizados, supervisados y realizados por funcionarios del Proceso de gestión de tecnología de información y comunicación de la Entidad. Si es necesario que un proveedor o contratista realice los cambios al paquete de Software, estos cambios serán realizados bajo el permiso y supervisión de la misma área, con la finalidad de garantizar la confidencialidad e integridad de la información contenida en los computadores, dispositivos móviles, sistemas de información y procesamiento a los que sea necesario realizarle cambios.

1.5.19.7. Pruebas de seguridad de sistemas.

Para los Sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba, para aceptación y criterios de aceptación, relacionados por parte del Proceso de gestión de tecnología de información y comunicación de la Entidad.

Con la finalidad de garantizar la disponibilidad de la información, se deben realizar las siguientes pruebas:

- **a.** Pruebas de compatibilidad: Se debe garantizar el funcionamiento adecuado y continúo del software desarrollado en diferentes plataformas: hardware, sistemas operativos, redes.
- **b.** Pruebas de integración: Se deben comprobar las conexiones y comunicaciones entre los diferentes módulos del software desarrollado y los demás sistemas de información de la Entidad que tengan relación con el desarrollo.
- **c.** Pruebas de función: Esta prueba permite asegurar que el sistema cumple con la funcionalidad para el cual fue hecho, con las especificaciones técnicas esperadas y es útil para los funcionarios de la Entidad.
- **d.** Pruebas de desempeño: La finalidad de esta prueba está orientada a establecer la eficiencia del sistema de información cuando es utilizado por parte de los funcionarios de la Entidad, estableciendo posibles fallas antes de su puesta en marcha.
- **e.** Pruebas de instalación: Esta prueba consiste en instalar el sistema de información en el servidor que alojará la base de datos o los archivos fuente del sistema de información.

1.5.20. POLÍTICA PARA LA ADQUISICIÓN, DISPOSICIÓN, IMPLEMENTACIÓN Y PUESTA EN MARCHA DE SERVICIOS Y APLICACIONES EN LA NUBE (CLOUD).

1.5.20.1. Preliminar y antecedentes.

Con fundamento en las disposiciones y lineamientos de la Guía 12. Seguridad en la Nube, que sustenta el Modelo de Seguridad y Privacidad de la Información (MSPI) y el NIST (National Institute of Estandards and Technology), el MINENERGÍA, progresivamente debe prever, adoptar, establecer e implementar mecanismos para la adquisición, disposición, implementación y puesta en marcha de servicios en la nube, en forma segura, reduciendo y minimizando los riesgos que la información puede, podría y llegaría a tener al dejarlas en custodia a un tercero que no es visible físicamente, pues este nuevo dominio le corresponde al ciberespacio.

El nuevo concepto de computación derivado de los nuevos servicios que se sustentan en la red de redes (Internet) y la World Wide Web (la Web) o red informática mundial, ha hecho que, por la facilidad de acceso y disponibilidad de la información, se puede acceder a cualquier momento y en cualquier ubicación del globo terráqueo.

Lo anterior, requiere de un nuevo reordenamiento internacional donde se requiere dar un estricto cumplimiento a nuevos requerimientos, requisitos, acuerdos de niveles de servicio entre las partes (entidades de la administración pública, dueños de la información y proveedores avalados, autorizados y certificados de servicios en la nube), con el acopio de la legislación local, regional y mundial, a través de la aplicación de estándares, recomendaciones de los organismos, entes autorizados y las buenas prácticas, que permitan garantizar siempre, entre otras cosas: la autenticidad, integridad, disponibilidad, no repudio, y en algunos casos, la privacidad de la información.

1.5.20.2. Análisis y especificación de requisitos de seguridad en la nube.

Acorde con los modelos de servicio vigentes en la nube, el MINENERGÍA establecerá los requisitos relacionados con la seguridad de la información, que irán intrínsecamente relacionados y sujetos con las especificaciones, requerimientos y necesidades de la aplicación, sistema de información, plataformas e infraestructura sobre las que se sustente más el acopio, ajuste y consenso de los acuerdos de niveles de servicio ofrecidos por el proveedor del servicio en la nube.

1.5.20.3. Identificación y análisis de riesgos inherentes a servicios en la nube.

El MINENERGÍA, acordará con los proveedores de servicios en la nube la estrategia y mecanismos y actividades asociadas para la migración a la nube, teniendo en cuenta si lo que se requiere colocar allí corresponde a: datos, servicios, aplicaciones, funcionalidades o procesos (Web Services y/o micro sitios), teniendo en cuenta los activos de información a mover, trafico presente y operaciones involucradas, valorando en todo caso, las variables de impacto, tales como: exposición del activo de información públicamente, acceso del activo por un encargado del tercero y/o proveedor del servicio, modificación de un proceso, por parte de un externo, entrega de resultados erróneos en un proceso o parte de su funcionalidad, modificación de datos e información de manera inesperada, o fallas de disponibilidad. Todo ello, al ser Cloud Computing en un modelo que proporciona acceso a unos recursos de computación configurable, esto es redes, servidores, almacenamiento, aplicaciones y servicios, que no dependen del quehacer diario del ambiente computacional tradicional, sino de un proveedor que oferta sus servicios para absolutamente cualquier ambiente corporativo que así lo requiera.

1.5.20.4. Aspectos de seguridad de la información para tener en cuenta en la nube.

Independientemente de la modalidad de servicio en la nube a adquirir (pública, privada, comunitaria o híbrida), los límites y requerimientos de seguridad pueden variar mucho de los que se tengan en el MINENERGÍA, y en tal sentido, su implementación deberá abordar no solo el contexto "interno" y "externo" en lo que respecta a la ubicación física de los activos, los recursos y la información, sino también por quienes están siendo usados, así como quién es responsable de su gobierno, seguridad y cumplimiento con las políticas y estándares.

Ejercicio que se debe complementar con: clasificación de los activos y los servicios de la entidad, planificación de la arquitectura de seguridad, de tal manera que se ajuste con los objetivos de la entidad, la regulación y el cumplimiento legal (análisis GAP), es decir, hacerle exigible al proveedor que el Ministerio traslada sus servicios a esta nueva modalidad de operación tecnológica, proporcionando los requerimientos mínimos de seguridad que se tienen localmente, más los acuerdos de niveles de servicio ofertados y ajustados, según los necesidades, requerimientos, y proyecciones futuras de la entidad, es decir, una conjugación de los requerimientos mínimos exigidos por la entidad en términos de seguridad y salvaguarda de la información dejada en custodia, con alcance y cumplimiento a plenitud de los acuerdos de niveles de servicio dispuestos por el operador a cargo.

De otro lado, será primordial que el proveedor de servicio en la nube pueda cumplir cabalmente con el ciclo de vida de la seguridad de los datos que corresponde a: la creación, el almacenamiento, el uso, el archivo y la destrucción.

1.5.21. POLÍTICA DE TELETRABAJO

El lugar en el cual se llevarán a cabo las actividades de teletrabajo debe contar con la protección física adecuada contra hurto, daño o pérdida del equipo y/o de la información, divulgación no autorizada de información, acceso remoto no autorizado a los sistemas de información de la Entidad o un mal uso de estos.

El Oficial de Seguridad de la Información y/o quien haga sus veces, debe verificar que las instalaciones donde se realicen las actividades de teletrabajo resguarden adecuadamente los equipos e información requeridos, así como los mecanismos de seguridad para garantizar la integridad, disponibilidad y confidencialidad de la información.

Política que de ninguna manera puede entenderse o constituirse como una barrera para la puesta en marcha del teletrabajo.

1.5.22. POLÍTICA DE RECURSO HUMANO.

Se debe garantizar la firma de un acuerdo de confidencialidad antes de iniciar labores o actividades dentro del MINENERGÍA para todas las partes interesadas, el cual se hace extensivo a aquellos proveedores críticos que tengan acceso a la información reservada de la Entidad.

Se debe divulgar y capacitar anualmente a todas las partes interesadas cuando se vinculan o ingresan al MINENERGÍA, en temas de seguridad de la Información, en los diferentes

procedimientos de protección de la información existente en la Entidad y el resultado de la implementación del SGSI en el MINENERGÍA. Así mismo lograr el compromiso y adaptación de una cultura basada en riesgos de Seguridad de la Información, para lo cual se puede consultar al Oficial de Seguridad de la Información en caso de duda o desconocimiento de un procedimiento formal de seguridad, ya que esto no exonerará del proceso disciplinario, correspondiente a las violaciones de las políticas o normas de Seguridad de la Información que existan publicadas en el sistema de información SIGME del MINENERGÍA.

1.5.23. POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES.

Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación del negocio. El Ministerio de Minas y Energía planea, gestiona, respalda y monitorea la infraestructura tecnológica siguiendo los lineamientos establecidos en los procedimientos establecidos para el SGSI.

1.5.24. POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

El Ministerio de Minas y Energía establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación.
Antes de Iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesario durante y después del contrato.

1.5.25. POLÍTICAS DE CUMPLIMIENTO

El Ministerio de Minas y Energía velará por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública.

GLOSARIO:

i. **Activo de información:** cualquier recurso de valor para el MINENERGÍA, representado en una persona, proceso o tecnología aplicada, de relevancia e importancia que le permiten cumplir con su rol misional, funcional y operacional. (MINENERGÍA)
ii. **Áreas seguras:** zonas, sitios o locaciones delimitadas con esquemas, sistemas y mecanismos de seguridad (física, electrónica, digital y/o combinada), donde se salvaguardan y protegen activos críticos de una organización, restringiendo su acceso únicamente al personal autorizado, quien está sujeto a protocolos de acceso, vigilancia y control. (MINENERGÍA)
iii. **Dueño del proceso:** hace referencia a la persona, dependencia, funcionario, servidor público, contratista que tiene a su haber actividades o funciones directamente relacionadas con la razón de ser de un proceso o dependencia clave dentro del MINENERGÍA. (MINENERGÍA)
iv. **Firma de pie de página:** corresponde a la información al final de cada correo electrónico, donde se identifican los campos de: nombre de la persona que escribe y envía el correo, cargo, profesión, Entidad a la que pertenece, dirección, teléfonos (fijo y móvil), ciudad y país, entre otros. (MINENERGÍA)
v. **Hacktivismo:** acrónimo de hacker y activismo. Hace referencia a "la utilización no-violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos. Estas herramientas incluyen desconfiguraciones de los portales web, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollo de software". A menudo se entiende por la escritura o reescritura de programas informáticos, a efectos de directa o indirectamente promover o privilegiar una ideología política, y por lo general potenciando estrategias o políticas tales como libertad de expresión, derechos humanos, y ética de la información. (MINENERGÍA)
vi. **Líderes funcionales:** personal que tiene el rol temático dentro las tareas y actividades propias de su dependencia, que conoce en esencia la razón de ser de función dentro de su proceso, sustentada en sus conocimientos, competencias, habilidades, destrezas, experticia, y que además tiene dominio sobre la herramienta TIC de su resorte o dominio, si aplica. (MINENERGÍA)

vii. **Información crítica:** hace referencia a aquellos activos de información (física, impresa o digital), documentos, proyectos, sistemas de información y hasta recursos humanos, que son vitales y de suma importancia, para la gestión misional y operacional del MINENERGÍA. (MINENERGÍA)

viii. **Información etiquetada:** información que en algún momento puede ser o estar en el estado de privada, clasificada o reservada y para su control y manejo (copia, publicación) deberá mediar un permiso o autorización especial de su dueño o custodio. (MINENERGÍA)

ix. **Oficial de Seguridad de la Información:** dentro de una organización, el Oficial de Seguridad de la Información o Director de Seguridad de la información, del inglés, CISO(Chief Information Security Officer: 'oficial principal de seguridad de la información'), es el responsable máximo en planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar la Seguridad de la Información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad.

x. Los obstáculos y los riesgos de seguridad que las organizaciones confrontan se resuelven con la misma velocidad con los que surgen nuevos, más complejos. El oficial de Seguridad de la Información, responsable de proteger los negocios del impacto de esos riesgos, necesita de políticas, productos y servicios para dirigir el desafío de mantener la seguridad. (MINENERGÍA)

xi. **Partes interesadas:** en el presente contexto, se refiere a dos actores: a) El MINENERGÍA, con la Alta Dirección a la cabeza, sus delegados o designados en su representación, y b) funcionarios y/o servidores públicos, contratistas, proveedores, operadores TIC al servicio del MINENERGÍA, stakeholders. (MINENERGÍA)

xii. **Proveedores críticos:** son aquellas Entidades (personas jurídicas) o personas naturales que bajo cualquier modalidad de contratación se encuentran vinculadas con el MINENERGÍA, prestando un servicio básico y/o esencial para la funcionalidad y operación de alguno de sus procesos, y donde se les ha delegado, entregado o dejado en custodia parte de sus activos de información relevante o crítica, para el cumplimiento de las labores encomendadas. (MINENERGÍA)

xiii. **Redes externas:** cualquier otro vínculo, enlace, sitio web no referenciado o validado por la plataforma de seguridad TIC y fuera del alcance del dominio del MINENERGÍA. (MINENERGÍA)

xiv. **Responsable de área segura:** persona con conocimientos certificados y acreditados en temas de seguridad física e informática, seguridad de la información, ethical hacking, centros de datos seguros, zonas seguras, entre otros. (MINENERGÍA)

xv. **Terceros o proveedores:** es toda persona, proveedor, que está implicada directamente con vínculo contractual en el MINENERGÍA, y tiene a su cargo o responsabilidad el manejo y uso de información para el cumplimiento de las funciones y compromisos adquiridos. Los terceros, también se refiere a todas aquellas personas y/o organismos que interactúan e intercambian información con la Entidad a través de cualquiera de sus procesos vigentes. (MINENERGÍA)

xvi. **Usuarios:** Son los servidores públicos y contratistas del Ministerio de Minas y Energía, los terceros y los aliados de negocio.

Proyectó: Oscar Sánchez S. / Carlos Javier Osorio B.
Revisó: Juan José Cedeño López / Jorge Eliecer Lozano Espina / Feiber Alexander Ochoa / Jorge Eduardo Salgado Ardila
Aprobó: Nelson Javier Vásquez Torres