República de Colombia

Libertad y Orden

MINISTERIO DE MINAS Y ENERGIA

RESOLUCIÓN NÚMERO 0362 DE

(3 MAY 2017)

"Por la cual se adopta 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 las Políticas de Seguridad y Privacidad de la Información"

EL MINISTRO DE MINAS Y ENERGÍA

En ejercicio de sus facultades legales conferidas por el Decreto 381 de 2012, modificado y adicionado por el Decreto No. 1617 de 2013 y el numeral 3 de la Ley 489 de 1998,

CONSIDERANDO

Que la Ley 1341 de 2009, estableció el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, incorporando principios, conceptos y competencias sobre su organización y desarrollo e igualmente señaló que las Tecnologías de la Información y las Comunicaciones deben servir al interés general y, por tanto, es deber del Estado promover su acceso eficiente y en igualdad de oportunidades a todos los habitantes del territorio nacional.

Que el Decreto 1083 de 2015, adicionado por el Decreto 415 de 2016, establece la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones, cuyo ámbito de aplicación, de acuerdo con el artículo 2.2.35.2, corresponde a las entidades del Estado de orden nacional y territorial, los organismos autónomos y de control.

Que el artículo 2.2.35.3 del Decreto 1083 de 2015, adicionado por el Decreto 415 de 2016, establece como objetivos del fortalecimiento institucional: "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 así mismo, una de las metas que pretende alcanzar el Programa Visión Colombia 2019, es el cumplimiento del objetivo "UN ESTADO AL SERVICIO DE LOS CIUDADANOS", el desarrollo de la estrategia "AVANZAR HACIA UNA SOCIEDAD INFORMADA", la cual dispone que: *"En 2019 la información deberá ser un derecho efectivo y un instrumento de difusión y apropiación del conocimiento, que promueva el desarrollo económico, la equidad social y la democracia. En ese contexto, Colombia deberá alcanzar estándares adecuados de generación de información confiable y oportuna, y de uso colectivo. El Estado promoverá su diseminación, aprovechando el uso de las tecnologías de la información y las comunicaciones"*, cumpliendo con los estándares de gobierno, en especial los establecidos con relación **a la seguridad** que

hace parte de los cuatro pilares: TIC para Servicios, TIC para datos abiertos, TIC para la Gestión y TIC para la seguridad.

Que mediante el Decreto 2573 de 2014, "*Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea*", se describen los lineamientos, se incorporan mejores prácticas y se orienta la implementación para lograr una administración pública más eficiente, coordinada y transparente, a través del fortalecimiento de la gestión de las Tecnologías de la Información y se reglamenta el Marco de Referencia de Arquitectura Empresarial para Entidades del Estado, el cual es un modelo de referencia puesto a disposición del Estado Colombiano para servir como orientador estratégico de las arquitecturas empresariales, lo cual debe estar articulado con los lineamientos de seguridad de la información.

Que el Artículo 2.2.9.1.2.1 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones 1078 de 2015, establece como cuarto componente, para desarrollar los fundamentos de la estrategia que facilitarán la masificación de la oferta y la demanda del Gobierno en Línea, el de la **Seguridad y privacidad de la Información.**

"Que el Modelo de Seguridad y Privacidad de la Información (MSPI), versión 3.0 de fecha 03/03/2015 adoptado por el Ministerio de Tecnologías de la Información y las Comunicaciones, reúne el conjunto de lineamientos, políticas, normas, procesos e instituciones que proveen y promueven la puesta en marcha, supervisión, mejora y control de la implementación del modelo, así como la implementación de la Estrategia de Gobierno en Línea, establecida en el manual GEL. Esta nueva estrategia, que se plasma en el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones 1078 de 2015, comprende cuatro grandes propósitos: lograr que los ciudadanos cuenten con servicios en línea de muy alta calidad, impulsar el empoderamiento y la colaboración de los ciudadanos con el Gobierno, encontrar diferentes formas para que la gestión en las entidades públicas sea óptima gracias al uso estratégico de la tecnología y garantizar la seguridad y la privacidad de la información de la entidad.

Que el mencionado MSPI del MINTIC, se fundamenta en los lineamientos de las Normas Continuidad del negocio SGCN (Norma ISO/IEC 22301:2012), y seguridad de la información SGSI (Normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013).

Que en aplicación de lo dispuesto por el artículo 2.1.2.1.23 del Decreto 1081 de 2015, adicionado por el artículo 5º del Decreto 270 de 2017, el presente proyecto de reglamentación fue publicado en la página web del Ministerio de Minas y Energía, por un término de quince (15) días calendario contados a partir del 6 del mes de abril de 2017 y hasta el 21 del mes de abril del mismo año, con lo cual, adicionalmente, se surte lo dispuesto por el numeral 8 del artículo 8° de la Ley 1437 de 2011.

Que en Mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1º. Objeto. Adoptar la Política General de Seguridad y Privacidad de la Información, Política de Tratamiento y Protección de Datos Personales, Política de Continuidad del Negocio, y Políticas de Seguridad y Privacidad de la Información en el Ministerio de Minas y Energía como norma fundamental para el desarrollo de proyectos de tecnología con una gestión eficiente y optimización de los recursos, servicios TIC, y los sistemas de información.

ARTÍCULO 2º. Ámbito de Aplicación. Las políticas aplican a los servidores públicos, contratistas, proveedores y/o terceros usuarios de la información impresa, digital, y la soportada sobre las tecnologías de información y las comunicaciones del Ministerio de Minas y Energía.

ARTÍCULO 3º Políticas. La presente Resolución adopta las siguientes políticas, que se describen en el documento anexo:

"Por la cual se adopta 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 las Políticas de Seguridad y Privacidad de la Información"

Política General de Seguridad y Privacidad de la Información, en cumplimiento del numeral 5.2 de la Norma ISO/IEC 27001:2013.

Política de Tratamiento y Protección de Datos Personales, en cumplimiento de los lineamientos de la Ley 1581 de 2012.

Política de Continuidad del Negocio o del Sistema de Gestión y Continuidad del Negocio (SGCN), en cumplimiento de la Norma ISO/IEC 22301:2012, y el numeral A.17, Anexo A de la Norma ISO/IEC 27001:2013

Política de Recuperación ante Desastres TIC, en cumplimiento de la Norma ISO/IEC 22301:2012

Políticas de Seguridad y Privacidad de la Información, en cumplimiento de los requerimientos del numeral A.5, Anexo A de la Norma ISO/IEC 27001:2013.

ARTÍCULO 4° 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 5° Conformación de las Mesas de Trabajo y Funciones.

1. 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 MSPI y el SGSI, a través de un equipo de trabajo conformado por un representante de las siguientes áreas o dependencias del Ministerio de Minas y Energía:

- Despacho del Señor Ministro.
- Secretaría General.
- Oficina de Planeación y Gestión Internacional.
- Oficial de Seguridad de la Información.
- Subdirección de Talento Humano.
- Oficina de Control Interno.
- Grupo de Tecnologías de la Información y la Comunicación.
- Subdirección Administrativa y Financiera.
- Grupo de Procesos Misionales
- Grupo de Servicio al Ciudadano

La Mesa de Trabajo de Seguridad y Privacidad de la Información está liderada por el Oficial de Seguridad de la información; sin embargo, los miembros tendrán las siguientes funciones según su competencia, sin perjuicio de las establecidas en las políticas:

- Tomar decisiones que requiera el MSPI y el SGSI y las propuestas que lleve el Oficial de Seguridad de la Información y cualquiera de sus miembros, respecto a los riesgos y a la seguridad de las informaciones requeridas para la Entidad.

- 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 MSPI de la Entidad.

- 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 SGSI y del MSPI.

- Desarrollar y liderar la implementación de métricas de seguridad adecuadas para evaluar la efectividad y desempeño del SGSI y el MSPI.

- Diseñar, sugerir o promover nuevas estrategias para la gestión de riesgos detectados.

- Conocer y analizar alertas globales de seguridad y determinar planes de acción para el tratamiento de las mismas.

- Mantener informado a todos las partes interesadas sobre la gestión macro del MSPI, de la entidad de manera periódica.

2. Mesa de Trabajo de Gestión de Cambios y Continuidad del Negocio. La Mesa de Trabajo de Gestión de Cambios y Continuidad del Negocio, tendrá a su haber todas 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 SGCN, y el SGSI, a través de un equipo de trabajo conformado por un representante de las siguientes áreas o dependencias del Ministerio e de Minas y Energía:

- Despacho del Señor Ministro.
- Secretaría General.
  Oficina de Planeación y Gestión Internacional.
- Oficial de Continuidad del Negocio.
- Subdirección de Talento Humano.
- Oficina de Control Interno.
- Grupo de Tecnologías de la Información y la Comunicación.
- Subdirección Administrativa y Financiera.
- Procesos Críticos avalados por el BIA vigente en el Ministerio, sujetos a un Plan de Continuidad del Negocio.

La Mesa de Trabajo de Gestión de Cambios y Continuidad del Negocio está liderada por el Oficial de Continuidad del Negocio; sin embargo, los miembros tendrán las siguientes funciones según su competencia, sin perjuicio de las establecidas en las políticas:

- Tomar decisiones que requiera el SGCN y las propuestas que lleve el Oficial de Continuidad del Negocio y cualquiera de sus miembros, respecto a los riesgos y temas de Continuidad del Negocio requeridos para la entidad.

- 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.

- 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).

- 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).

- Diseñar, sugerir o promover nuevas estrategias para la gestión de riesgos detectados.

- Conocer y analizar alertas globales de Continuidad del Negocio y determinar planes de acción para el tratamiento de las mismas.

- Mantener informado a todas las partes interesadas sobre la gestión macro del Sistema de Gestión de Continuidad del Negocio (SGCN) de la entidad de manera periódica.

- Velar por que los programas de concientización en Continuidad del Negocio se lleven a cabo según lo planeado.

- Asegurar que la adaptación al cambio del personal de base versus el personal crítico preparado y formado para atender un plan de contingencias, están apoyados planes de sensibilización, capacitación, compromiso y sentido de pertenencia del rol a asumir ante la materialización de un evento o hecho inesperado.

ARTÍCULO 6º. Vigencia. La presente Resolución rige a partir de su publicación.

PUBLÍQUESE Y CÚMPLASE

Dado en Bogotá D.C., a los - 3 MAY 2017

GERMÁN ARCE ZAPATA
Ministro de Minas y Energía

Elaboró: Óscar Sánchez Sánchez
Revisó: Laura Rocío Remolina Cabrera
Aprobó: Germán Eduardo Quintero Rojas

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES, POLÍTICA DE CONTINUIDAD DEL NEGOCIO, POLÍTICA DE RECUPERACIÓN ANTE DESASTRES TIC, y POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL MINISTERIO DE MINAS Y ENERGÍA

1 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración del **Ministerio de Minas y Energía,** con respecto a la protección de los activos de información integrados por los funcionarios y/o servidores públicos, contratistas, proveedores, la información como tal, los procesos, 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), 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.

Para asegurar la dirección estratégica de la Entidad, el **Ministerio de Minas y Energía,** establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos críticos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información (SGSI).
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas, proveedores, aprendices, practicantes y clientes del Ministerio de Minas y Energía.
- Garantizar la continuidad del negocio frente a incidentes. Alcance/Aplicabilidad

- Esta política aplica a toda la entidad, sus funcionarios, servidores públicos, contratistas y proveedores del Ministerio de Minas y Energía, y la ciudadanía en general.

Nivel de Cumplimiento de la Política

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

A continuación se establecen las doce (12) políticas de seguridad que soportan el MSPI y el SGSI del **Ministerio de Minas y Energía**:

1. **El Ministerio de Minas y Energía** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información (SGSI), soportado en lineamientos claros alineados a las necesidades del negocio 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 5 del presente documento, deberán ser compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o proveedores.
3. **El Ministerio de Minas y Energía** protegerá la información generada, procesada o resguardada por los procesos críticos de negocio y activos de información que hacen parte de los mismos.
4. **El Ministerio de Minas y Energía** 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. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. **El Ministerio de Minas y Energía** protegerá su información de las amenazas originadas por parte del personal.
6. **El Ministerio de Minas y Energía** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. **El Ministerio de Minas y Energía** controlará la operación de sus procesos críticos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
8. **El Ministerio de Minas y Energía** implementará control de acceso a la información, sistemas y recursos de red.
9. **El Ministerio de Minas y Energía** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10. **El Ministerio de Minas y Energía** garantizará, a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información, una mejora efectiva de su modelo de seguridad.

11. **El Ministerio de Minas y Energía** garantizará la disponibilidad de sus procesos críticos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
12. **El Ministerio de Minas y Energía** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

2 POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES.

El **MINMINAS** conforme a lo establecido en la normatividad vigente, define lo siguiente:

Ámbito de aplicación: Aplica a todos los procesos del **MINMINAS**.

Excepción al ámbito de aplicación de las políticas de tratamiento de datos personales:

Se llevara a la Mesa de Trabajo de Seguridad y Privacidad de la Información, anexa al Comité del Modelo Integrado de Planeación y Gestión cualquier excepción a la política para la toma de decisiones respectiva.

Principios del tratamiento de datos personales a cumplir por el **MINMINAS**:

- **Principio de la Legalidad**: El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
- **Principio de finalidad**: Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.
- **Principio de libertad**: El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.
- **Principio de veracidad o calidad**: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- **Principio de transparencia**: Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.
- **Principio de acceso y circulación restringida**: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.
- **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.
- **Principio de confidencialidad**: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva y confidencialidad de dicha información.

Derechos de los titulares: La política indica los derechos de los titulares de los datos, tales como:

- Conocer, actualizar y rectificar sus datos personales.
- Solicitar la prueba de su autorización para el tratamiento de sus datos personales.

- Ser informado respecto del uso que se le da a sus datos personales.
- Revocar la autorización y/o solicitar la supresión de sus datos personales de las bases de datos o archivos cuando el titular lo considere, siempre y cuando no se encuentren vigentes con la entidad los servicios o productos que dieron origen a dicha autorización.
- Presentar quejas ante la entidad administrativa encargada de la protección de los datos personales.

Autorización del titular: La política indica cómo obtener autorización del titular para el tratamiento de sus datos personales, así como los casos en los cuales no se requiere autorización del titular.

Deberes de los responsables del Tratamiento: La política indica cuales son los deberes de los responsables y/o encargados del tratamiento de los datos personales, para lo cual debe contener un compromiso o acuerdo de uso y manejo de la información entregada bajo su custodia, a través del cual todo funcionario, contratista y/o proveedor vinculado a la Entidad, deberá firmar un compromiso de no divulgar la información interna y externa que conozca de la Entidad, así como la relacionada con las funciones que desempeña en la misma.

La firma del acuerdo implica que la información conocida por todo funcionario y/o servidor público, contratista y/o proveedor, bajo ninguna circunstancia debe ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización del titular, dueño o dependencia a cargo La política indica desde cuando se firma el acuerdo de confidencialidad, así como la vigencia del mismo.

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

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

El Ministerio de Minas y Energía (MINMINAS) 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 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 Ministerio de Minas y Energía 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.

Dentro del compromiso de la Alta Dirección del Ministerio de Minas y Energía, se encuentra el de la revisión periódica de esta política y de todo el Sistema de Gestión de Continuidad del Negocio y el de mejorarlo continuamente brindando todo el apoyo a los responsables de gestionarlo.

Objetivos de la continuidad del negocio y planes para alcanzarlos

La Alta Dirección del 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 permita alcanzar los objetivos de continuidad de negocio.

Para tal fin, el Ministerio acoge los siguientes objetivos de Continuidad del Negocio:

- Continuar con las operaciones del Ministerio y sus servicios críticos a un nivel de servicio aceptable que permita cumplir con sus obligaciones legales y contractuales.
- Minimizar la exposición del Ministerio a sanciones legales por incumplimiento con las partes interesadas.

- Mitigar los efectos negativos que puedan producirse en los planes estratégicos del Ministerio.
- Mantener la reputación e imagen del Ministerio.

El Ministerio de Minas y Energía debe determinar quién será el responsable de cada objetivo, que hará para lograrlo que recursos

4 POLÍTICA DE RECUPERACIÓN ANTE DESASTRES

Objetivo, alcance y usuarios

El propósito de esta política es definir el objetivo, alcance y reglas básicas para la Gestión de la continuidad de la operación de Tecnologías de Informática y Comunicaciones del Ministerio de Minas y Energía – **MINMINAS**.

Esta política se aplica a todo el Sistema de Gestión de la Continuidad de la operación de TIC del **MINMINAS**, pero en particular al Sistema de Recuperación ante Desastres (DRP, por su sigla en inglés)

Los usuarios de este documento son todos los empleados del Grupo TIC del **MINMINAS**, así como también todos los proveedores y socios que cumplen alguna función con la operación de tecnologías de información y comunicaciones de la Entidad.

Documentos de referencia

- Norma ISO/IEC 22301 de 2012
- Norma ISO/IEC 27001:2013
- Manual para la Recuperación de Desastres de los Servicios que presta el Grupo TIC del **MINMINAS**

Gestión de la Continuidad de la Operación de TIC

Objetivo

El objetivo de la Gestión de la Continuidad de la Operación de TIC es 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.

Alcance

La Gestión de la Continuidad de la Operación de TIC se implementa para la Gestión Tecnológica de Información y Comunicación del Ministerio de Minas y Energía, con especial atención sobre las actividades identificadas como críticas durante el Análisis de impactos en el negocio.

Las ubicaciones de Operación de TIC del MME incluidas en el alcance:

- Sede Principal Calle 43 No. 57-31 CAN

Unidades organizativas incluidas en el alcance:

- Grupo TIC – Secretaría General

Premisa

Partiendo de la premisa que el **MINMINAS** no cuenta con un Sistema de Gestión de Continuidad de Negocio - SGCN formal, esta política hace parte del Plan de Recuperación Ante Desastres de TIC (DRP – TIC), el cual a su vez hace parte del Plan de Continuidad de Tecnología – (PC-TIC) que deberá ser implementado por el Ministerio.

Productos y Servicios Clave

Los siguientes productos y servicios clave son suministrados por la gestión del grupo TIC dentro del alcance definido en la sección anterior.

Los Sistemas de Información Críticos y el entorno tecnológico que se requiere para su normal operación, corresponden:

- Sistema de Información de Combustibles Líquidos – SICOM (Entregado a un Tercero bajo el esquema de administración delegada y hosting de infraestructura HW y SW a nivel de producción y contingencia)
- Directorio Activo
- Portal WEB
- Sistema de Correspondencia y Fondos Acumulados P8
- SARA
- SI.MINERO
- SIGME-TMS
- NEON
- SUIME3
- GLP

La Gestión de la Continuidad de la Operación de TIC debe garantizar que los productos mencionados precedentemente se recuperarán a un nivel predefinido.

Responsabilidades para la Gestión de la Continuidad de la Operación de TIC

Responsabilidades generales:

- **El Administrador del Centro de Cómputo** es el responsable de garantizar que la Gestión de los Planes de Recuperación Ante Desastres TIC sean implementados de acuerdo con esta política y de garantizar los recursos necesarios.

- **El Outsourcing de Administración tecnológica del Ministerio de Minas y Energía** es responsable de la implementación operativa y del mantenimiento de la Gestión de los Planes de Recuperación Ante Desastres de TIC.

- El Grupo TIC debe revisar la Gestión de los Planes de Recuperación Ante Desastres de TI al menos una vez por año o cada vez que se produzca una modificación significativa, y debe elaborar un informe de la revisión y los simulacros del mismo, una vez implementado, por lo menos dos veces al año. El objetivo de la revisión es establecer la conveniencia, adecuación y eficacia de los Planes de Recuperación de Desastres implementados, en aras de lograr la funcionalidad del Sistema de Gestión de la Continuidad de la Operación de TIC.

- **El Secretario General del Ministerio de Minas y Energía** tiene la función de promover el desarrollo e implementación de programas sistematizados y asesorar al Ministro en la formulación de políticas, normas y y procedimientos para la administración de recursos humanos, físicos, económicos, financieros e informáticos del Ministerio. En este sentido, promueve que la gestión de la Continuidad de la Operación de TIC sea implementada bajo la presente política.

- **El Administrador del Centro de Cómputo y el Outsourcing de Administración Tecnológica del Ministerio de Minas y Energía** son responsables de la implementación operativa y del mantenimiento del Sistema de Gestión de la Continuidad de la Operación de TIC.

- El Grupo TIC debe revisar el Sistema de Gestión de la Continuidad de la Operación de TIC, al menos una vez por año o cada vez que se produzca una modificación significativa, y debe elaborar un informe de la revisión. El objetivo de la revisión es establecer la conveniencia, adecuación y eficacia de Sistema de Gestión de la Continuidad de la Operación de TIC, con el fin de apoyar eficientemente la funcionalidad del SGCN.

- La Mesa de Trabajo de Gestión de Cambios y Continuidad del Negocio del Ministerio de Minas y Energía debe revisar el SGCN al menos una vez por año o cada vez que se produzca una modificación significativa, y debe elaborar un informe de la revisión. El objetivo de la revisión por parte de la Mesa de Trabajo es establecer la conveniencia, adecuación y eficacia del SGCN.

Responsabilidades específicas:

- El **Administrador del Centro de Cómputo** es el responsable de adoptar e implementar el Plan de Capacitación y Concienciación que corresponde a todas las personas que cumplen una función en la Gestión de la Continuidad de la Operación de TIC.

- Los preparativos relacionados con la Continuidad de la Operación de TIC deben ser probados y verificados utilizando diversos métodos para establecer hasta qué punto son accesibles. Para ello, el **Administrador del Centro de Cómputo y el Outsourcing de Administración Tecnológica del Ministerio de Minas y Energía,** una vez se desarrollen las acciones que conlleven su implementación, deben redactar un Plan de prueba y verificación que debe ser aprobado por la Coordinación del Grupo TIC. Luego de cada prueba y verificación, debe elaborar un informe de implementación.

- El **Administrador del Centro de Cómputo y el Outsourcing de Administración Tecnológica del MINMINAS** son los responsables de adoptar e implementar el Plan de mantenimiento y revisión del Plan de Recuperación Ante Desastres de TIC para que todos los elementos de la Continuidad de la Operación de TIC estén operativos y actualizados.

- Cada vez que se activa un Plan de Contingencia, un Plan de Recuperación ante Desastres, o un Plan de respuesta a los incidentes, el **Administrador del Centro de Cómputo** es el responsable de supervisar la eficacia de la Gestión de la Continuidad de la Operación de TIC.

Comunicación de la Política

El **Coordinador del Grupo TIC** debe asegurarse de que todos los funcionarios y/o servidores públicos, contratistas del Grupo TIC y los Líderes Funcionales de los Servicios de TIC del MINMINAS, como también los proveedores que cumplen una función en la Gestión de la Continuidad de la Operación de TIC, estén familiarizados con esta política.

Validez y Gestión de Documentos

El propietario de este documento es el **Coordinador del Grupo TIC**, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de funcionarios y/o servidores públicos, contratistas, terceros y proveedores que no conocen este documento.
- No-conformidad de Gestión de la Continuidad de la Operación de TIC con disposiciones legales, obligaciones contractuales y demás documentos internos del Ministerio de Minas y Energía.
- Ineficacia de la implementación y mantenimiento la Gestión de la Continuidad de la Operación de TIC, se mide con base en los planes de pruebas y revisión de incidentes.
- Responsabilidades ambiguas para la implementación la Gestión de la Continuidad de la Operación de TIC.

5 POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.1 Política de Gestión de Activos

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

La información gestionada en todos los procesos del Ministerio de Minas y Energía, debe cumplir con lo siguiente:

- Asignar un responsable del activo de información, quien debe ser el líder funcional
- Mantener el Inventario de activos actualizado.
- Clasificar y proteger.
- De acuerdo con la clasificación de los activos y mecanismos de protección, determinar a quién se le permite el manejo de la información, el nivel de acceso a la misma y los procedimientos seguros para su adecuado tratamiento, el cual debe estar plasmado en un procedimiento formal.
- La clasificación de los activos se realizó de acuerdo al tipo de activo, 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.
- Los activos de información que contienen datos personales, deben estar en cumplimiento con la Ley 1581 de 2014.

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 **MINMINAS**. Es decir, no se pueden usar para propósitos diferentes para los cuales fueron definidos o para temas personales.

Las partes interesadas, aceptan no compartir las contraseñas o permitir el acceso no autorizado a las cuentas otorgadas para utilizar los servicios brindados por la Entidad y así mismo es responsable por el manejo adecuado de la información y las acciones que por mal uso se deriven de esos accesos.

Por lo tanto, se implementarán medidas adecuadas y se fortalecerá una cultura para reportar cualquier anomalía identificada, al Oficial de Seguridad de la Información, de acuerdo con los procedimientos establecidos, con el objeto de gestionar los riesgos e incidentes de seguridad que se puedan presentar en la entidad.

Se establece que los datos de acceso, son un elemento personal e intransferible, las partes interesadas asumen la responsabilidad sobre el buen o mal uso que se dé sobre los sistemas de información del **MINMINAS.**

La información del **MINMINAS**, debe ser respaldada de forma frecuente y de acuerdo a las políticas validadas y revisadas del SGSI, por el Oficial de Seguridad de la Información. Su almacenamiento debe estar en lugares apropiados y adecuados, en los cuales se garantice que la información está segura y podrá ser recuperada en caso de un desastre o de incidentes presentados.

El **MINMINAS** proporciona el hardware y el software requerido para los procesos de la entidad. Los datos e información creados, almacenados y recibidos, serán propiedad de la entidad; las partes interesadas, podrán realizar backup de sus archivos personales o de información pública, para poder copiar cualquier tipo de información etiquetada, para lo cual debe solicitar autorización al líder de proceso involucrado y con copia al Oficial de Seguridad de la Información.

La copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la entidad, serán sancionadas de acuerdo con las normas y legislación vigentes aplicables.

5.3 Política Uso Correo Electrónico

Toda comunicación por correo electrónico entre las partes interesadas, debe efectuarse mediante el uso del sistema aprobado por MINMINAS (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, éstos 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.

Todo correo saliente debe ir con firma de pie de página del remitente sin excepción.

En el caso de que se reciba una comunicación o correo electrónico sospechoso, de alguien desconocido o spam, debe reportarlo de inmediato, sin abrirlo, a la mesa de ayuda de Tecnologías de Información Institucional o al correo electrónico designado y divulgado para esta labor, que actualmente es jcarce@minminas.gov.co

El **MINMINAS** se reserva el derecho a monitorear, auditar y vigilar los correos electrónicos institucionales para garantizar que sea utilizado sólo 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 los mismos.

5.4 Política Uso de Internet

La utilización del servicio de internet ofrecido por el **MINMINAS**, debe estar limitado únicamente a asuntos laborales. 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.

El uso de redes sociales está restringido dentro de la Entidad, teniendo en cuenta que esto puede generar problemas de seguridad. La entidad debe garantizar que las dependencias responsables de publicar información institucional a través de estos medios lo pueda 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 **MINMINAS** 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.

No está permitido descargar programas sin autorización institucional, ni almacenar información personal.

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 al Ministerio, se deberá generar un procedimiento de clasificación de la información,

para que los propietarios de la misma 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.

La 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:

- **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.

- **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 esta Ley.

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.

- **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 esta Ley.

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.

5.6 Trae tu propio dispositivo (BYOD)

El acceso físico a las instalaciones del **MINMINAS**, 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 Informática del Contrato de Mantenimiento Preventivo y Correctivo vigente en la entidad (verbigracia SELCOMP), o quien haga sus veces, sin excepción.

Así mismo, se realizan campañas de sensibilización y concientización, acerca de las buenas prácticas de seguridad informática, equipos desatendidos y aseguramiento de los dispositivos para que estén en cumplimiento de los requerimientos mínimos de seguridad de la información, como por ejemplo un software de antivirus y actualizaciones de parches al día.

Responsabilidad por los dispositivos

- El **MINMINAS** no asume ninguna responsabilidad por los dispositivos personales de las partes interesadas que ingresen a la entidad.
- La entidad no asume ninguna responsabilidad por la información contenida en los dispositivos personales de las partes interesadas que ingresen a la entidad.
- Los dispositivos personales pueden estar sujetos a revisión o investigación en caso de ser necesario, previa firma autorizando el acceso al dispositivo por el propietario.
- El Grupo de TIC no proporcionará apoyo o soporte técnico alguno a dispositivos personales.

Uso responsable de tecnología

- Las partes interesadas deben usar contraseñas complejas, seguras y no compartirlas por ningún motivo.

- Si el dispositivo personal requiere conectarse a la red inalámbrica de la entidad, debe estar justificado el requerimiento, validado y aprobado por el Oficial de Seguridad de la Información, sin excepción.
- El software instalado en los dispositivos personales que hagan uso de los sistemas y/o activos de información de la entidad deben estar correctamente licenciados.
- Las partes interesadas deben cumplir con todas las políticas de seguridad de la información de MINMINAS.
- Se debe controlar los dispositivos personales mediante el uso de una herramienta o solución de administración de dispositivos móviles (del inglés, MDM) para la entidad.

5.7 Política Dispositivos Móviles

El **MINMINAS** controla, gestiona y aprueba el manejo de los dispositivos móviles (teléfonos inteligentes, portátiles, discos duros, USB, DVD) institucionales 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 tal caso se recomienda definir un procedimiento para que este control sea implementado y que requiera la aprobación por la Mesa de Trabajo de Seguridad y Privacidad de la Información.

- El Oficial de Seguridad de la Información definirá las opciones mínimas requeridas para la protección, configuraciones aceptables e instalación de antivirus para de los dispositivos móviles de la entidad.
- El Grupo TIC 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 TIC 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 TIC debe garantizar las copias de seguridad de la información contenida en los dispositivos móviles institucionales.
- Las partes interesadas deben evitar el uso de los dispositivos móviles institucionales en lugares que no les ofrezcan garantías de seguridad física para evitar pérdida o hurto.
- Las partes interesadas no deben modificar las configuraciones de seguridad, ni desinstalar software o instalar programas en los dispositivos móviles institucionales bajo su responsabilidad.
- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

- Se debe controlar los dispositivos personales mediante el uso de una herramienta o solución de administración de dispositivos móviles (MDM) para la entidad.

5.8 Política de Teletrabajo

El Oficial de Seguridad de la Información autorizará las actividades de teletrabajo cuando se implementen los controles de seguridad apropiados, de tal manera que se cumpla con la Ley 1221 de 2008 en el **MINMINAS** y las políticas de seguridad de la información definidas para el SGSI.

El lugar en el cual se llevarán a cabo las actividades de teletrabajo, deben 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 los mismos.

El Oficial de Seguridad de la Información debe verificar que las actividades 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.

Los equipos utilizados para el teletrabajo deberán contar como mínimo con la protección de antivirus, requisitos de barreras de firewall y demás soluciones requeridas para salvaguardar adecuadamente la información de la Entidad.

Se define con antelación entre el **MINMINAS** y las partes interesadas, el trabajo a realizar, la información y los sistemas a los que requiere acceder así como el horario al cual podrá acceder, el cual debe estar documentado y aprobado previamente por el Oficial de Seguridad de la Información.

El Oficial de Seguridad de la Información, realizará revisión periódica a las conexiones remotas sobre los sistemas de información y la plataforma tecnológica del **MINMINAS** y emitirá las recomendaciones respectivas para su ejecución y cumplimiento.

Actualmente el Oficial de Seguridad Informática está en cabeza de SELCOMP, compañía que tiene vigente el Contrato de Mantenimiento de la plataforma TIC de la entidad.

5.9 Política Pantalla y Escritorio Limpio

El **MINMINAS** 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 deben 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.

5.10 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 éstos realizan para la entidad.

Accesos de las partes interesadas (Usuarios)

- El Oficial de Seguridad de la información define los lineamientos para la configuración de contraseñas seguras que aplicaran sobre los usuarios en los todos los sistemas de información del **MINMINAS**, y la Mesa de Trabajo de Seguridad y Privacidad de la Información aprueba respectivamente, para lo cual se puede tener en cuenta aspectos como longitud, complejidad, cambio periódico cada 60 días, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

- Cada dueño de proceso o dependencia con copia al Oficial de Seguridad de la Información, debe realizar la solicitud al Grupo TIC para crear, modificar, bloquear

o eliminar 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.

- Los dueños de proceso deben definir los perfiles de usuario y roles y aprobar las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos y diligenciando la matriz de roles y perfiles requerida. Así mismo, deben verificar y ratificar semestralmente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

- Para las partes interesadas, no están autorizadas en compartir sus cuentas de usuario y contraseñas con otros usuarios, por lo que sí se detecta esta situación, será gestionado como un incidente de seguridad de la información y con las sanciones pertinentes.

5.11 Accesos a sistemas de información

- El dueño o jefe de cada dependencia del **MINMINAS**, debe aprobar el acceso a los sistemas de información que le competen, de acuerdo con la matriz de roles y perfiles establecida para los usuarios y validados por el Oficial de Seguridad de la información.

- El dueño de cada proceso debe monitorear periódicamente los roles y perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos y solicitar al Grupo TIC los cambios necesarios.

5.12 Política Manejo de Proveedores

Se establece mecanismos de control en las relaciones con los proveedores del **MINMINAS**, con el objetivo de asegurar el cumplimiento de todas las políticas, normas y procedimientos de seguridad de la información aplicables.

Las partes interesadas, responsables de la gestión de firma de contratos o convenios con los diferentes proveedores del **MINMINAS**, deben asegurar que se realice la adecuada divulgación, entendimiento y aceptación de las políticas, normas y procedimientos de seguridad de la información del **MINMINAS** a dichas partes sin excepción, esta política se puede anexar como un punto adicional en el contrato establecido y validado previamente por el Grupo de Gestión Contractual.

El Oficial de Seguridad de la información junto con la parte interesada responsable, realizará una visita anual al proveedor crítico, para revisar en sitio el cumplimiento de

la seguridad de la información del objeto contratado. Adicionalmente, realizará el respectivo seguimiento a los planes de acción y remediación en tiempos prudentes definidos en conjunto con el proveedor crítico.

Del mismo modo, se puede apoyar con la Oficina de Control interno, para solicitar acompañamiento en las visitas, con el fin de verificar el cumplimiento de todos los compromisos del proveedor crítico, y validar que estén de acuerdo con lo requerido por el **MINMINAS**.

5.13 Política Gestión de Riesgos

Se adopta al SGSI la guía para la administración del riesgo elaborado por el DAFP (Departamento Administrativo de la Función Pública)[1] para la gestión de riesgos integral para el **MINMINAS**, que así misma está basada en la ISO 31000 para la Gestión del Riesgo. A nivel interno se adoptará el Procedimiento Administración del Riesgo AG-P-05[2] de la entidad.

Los riesgos de seguridad de la información identificados en el **MINMINAS**, 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 **MINMINAS**.

Los riesgos de seguridad de la información, deben ser tratados en por la Mesa de Trabajo de Seguridad y Privacidad de la Información y evidenciar por medio de registros el seguimiento de los mismos, 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 **MINMINAS** previamente, para que tengan una base que sustente las inversiones y los beneficios o el tratamiento al riesgo establecido.

---

[1]La guía se puede consultar en el siguiente link:
http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba
[2]El procedimiento se puede consultar en el siguiente link:
https://www.minminas.gov.co/procesos-y-procedimientos → Mapa de Procesos → Proceso Estratégico "Administración del sistema integrado de gestión" → Consulta de Documentos

5.14 Política con terceras partes (Proveedores)

Se debe firmar sin excepción un acuerdo de confidencialidad entre ambas partes para proteger la información del MINMINAS, antes de iniciar la ejecución del mismo. El acuerdo debe definir claramente el tipo de información que intercambiarán las partes, los medios, la frecuencia y los procedimientos a seguir. El Oficial de Seguridad de la Información y la Oficina de Control Interno, valida que dichos acuerdos existan de manera periódica con los proveedores críticos del **MINMINAS**.

5.14.1 Durante la prestación del servicio

El Oficial de Seguridad de la Información debe verificar en el momento de la conexión y, cuando se considere pertinente, el cumplimiento de las condiciones de seguridad mínimas de los equipos tecnológicos y los dispositivos móviles de los proveedores críticos en la red de datos de la entidad.

El Oficial de Seguridad de la Información debe verificar las condiciones y configuraciones de comunicación segura, cifrado y transmisión de información desde y hacia los proveedores críticos de servicios.

Los supervisores y/o interventores de los contratos y con apoyo del Oficial de Seguridad de la Información, deben monitorear periódicamente los proveedores críticos de la entidad, revisar el cumplimiento de los acuerdos de niveles de servicio, los acuerdos de confidencialidad, los acuerdos de intercambio de información, procedimientos de entrega o eliminación de la información, gestión de riesgos y los compromisos de Seguridad de la Información para que se cumplan sin excepción.

5.15 Política de Recurso Humano

En toda vinculación de personal al **MINMINAS**, la Subdirección de Talento Humano debe verificar que la documentación anexa a la hoja de vida sea veraz y acorde al cargo requerido, especialmente para los cargos críticos de la entidad[3], también se recomienda realizar estudios previos de seguridad física, para las partes interesadas que por sus funciones, responsabilidades y acceso a la información clasificada como publica reservada lo ameriten.

Se debe garantizar la firma de un acuerdo de confidencialidad antes de iniciar labores o actividades dentro del **MINMINAS**, para todas las partes interesadas, el cual se hace

[3] Documento Consultoría: "Informe Análisis Impacto al Negocio_BIA V2.docx"

extensivo a aquellos proveedores críticos que tengan acceso a la información reservada de la Entidad.

Se debe divulgar y capacitar a todas las partes interesadas cuando se vinculan o ingresan al **MINMINAS** y anualmente en temas de seguridad de la información, en los diferentes procedimientos de protección de la información existente en la Entidad, resultado de la implementación del SGSI en el MINMINAS. 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 **MINMINAS**.

5.16 Política de Gestión de Incidentes de Seguridad

El **MINMINAS** 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 los mismos en la entidad.

Se asigna como responsable para la entidad de la gestión de los incidentes de seguridad al Oficial de Seguridad de la Información y la Mesa de Trabajo de Seguridad y Privacidad de la Información para toma de decisiones, quienes deben asegurar que se realiza una adecuada evaluación del impacto en el Ministerio, de los incidentes de seguridad presentados y 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.

La Alta Dirección es la única dependencia autorizada para reportar los incidentes de seguridad de la información ante las autoridades competentes previa validación de la Oficina Asesora Jurídica del **MINMINAS**, así como de hacer pronunciamientos oficiales a las partes interesadas.

Cualquier parte interesada debe informar los incidentes de seguridad de la información que identifique o que reconozca su posibilidad de materialización, para lo cual se informa vía telefónica, correo electrónico o de manera verbal al Coordinador del Grupo TIC del **MINMINAS**, quien a través del Oficial de Seguridad Informática, rol actualmente vigente en el Contrato de Mantenimiento vigente, se prioriza su recepción, tratamiento

y solución, acorde con el uso de las buenas prácticas y recomendaciones para estos casos. A nivel transversal y para contemplar no solo, el tratamiento y manejo de los incidentes informáticos, sino también los eventos relacionados con incidentes de información que no son digitales o electrónicos, será implementado un procedimiento, avalado por Oficial de Seguridad de la Información y la Oficina de Control Interno, por los canales destinados para ello, que le permita a la entidad contar con una herramienta o mecanismo de registro canalización, trazabilidad y solución apropiada para este fin.

El Oficial de Seguridad de la Información y la Mesa de Trabajo de Seguridad y Privacidad de la Información del **MINMINAS**, deben registrar todos los incidentes presentados, gestionar métricas y generar recomendaciones de mejora sobre los mismos, con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros.

Los incidentes de seguridad de la información reportados y gestionados deben ser presentados a la Mesa de Trabajo Administrativo Institucional de manera trimestral, para la toma de decisiones y seguimiento de cierre o solución de manera oportuna y eficaz.

Se recomienda al **MINMINAS** adoptar la ISO 27035:2011 referente a la implementación de los procedimientos de Gestión de Incidentes de Seguridad necesarios para evidenciar calidad y mejora continua al respecto, tales como:

- ✓ Identificar, comunicar y evaluar los incidentes de la seguridad de la información.
- ✓ Contestar, gestionar los incidentes de la seguridad de la información.
- ✓ Identificar, examinar y gestionar las vulnerabilidades de seguridad de la información.
- ✓ Aumentar la mejora de la continuidad de la seguridad de la información y de la gestión de los incidentes, como respuesta a la gestión de incidentes de la seguridad de la información y de las vulnerabilidades en el **MINMINAS**.

5.17 Política Gestión del Cambio

El **MINMINAS** garantiza 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 del **MINMINAS**, debe ser solicitado o notificado formalmente

al Grupo TIC previamente para su validación y se aprobará por el dueño del proceso afectado en el cambio.

El **MINMINAS** conforma una Mesa de Trabajo de Cambios para la entidad, 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 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 afectados, 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.

5.18 Política Respaldo y Copias de Seguridad

El **MINMINAS** garantiza la generación continua de 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 del **MINMINAS** se debe realizar de manera interna y externa, de acuerdo a 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 debe reportar los resultados al Oficial de Seguridad de la Información y a la Oficina de Control Interno.

Nota: Actualmente, las cintas de los backups de respaldo se guardan en la Cintoteca del Archivo Central, a la cual se le invirtieron recursos importantes para que cumpliera con los estándares mínimos.

5.19 Políticas de Eliminación y Destrucción de Información

El **MINMINAS** 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.

La eliminación segura de medios físicos (USB, Discos duros, entre otros), se puede realizar con diversos mecanismos técnicos tales como: sobre-escritura, desmagnetización o destrucción física. De acuerdo al medio, se establece la herramienta adecuada y el procedimiento a seguir, tanto de información en medio físico o lógico, se recomienda en la fase de implementación aplicar un procedimiento, basado en las mejores prácticas según las directrices de NIST 800-88, referente al borrado seguro de datos.

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 por el proveedor de alistamiento de equipos.

5.20 Política Transferencia de Información y Cifrado

El **MINMINAS** asegura la protección de la información en el momento de ser transferida o intercambiada internamente 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:

- Responsabilidades y procedimientos para controlar la transmisión y recepción de información.
- Procedimientos para garantizar la trazabilidad y no repudio.
- Responsabilidades en caso de incidentes de seguridad de la información.
- Políticas, procedimientos y normas para proteger la información y los medios contenedores.
- Prohibición de divulgar la información entregada.
- 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 hacen parte de la operación del **MINMINAS**, 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.

La información pública clasificada y pública reservada en medio impreso o físico, debe permanecer en cajones cerrados bajo llave, entrega en mano, embalaje con sellos de seguridad, entre otros mecanismos de seguridad requeridos para proteger la información allí contenida.

Las partes interesadas deben evitar tener conversaciones confidenciales sobre información de la entidad en lugares públicos, oficinas abiertas, ascensores y lugares de reunión social para evitar la escucha o interceptación de información no autorizada.

No está permitido el intercambio de información pública clasificada y reservada de la entidad, por medio telefónico o por correo electrónico, sin las debidas protecciones y controles necesarios que la ameritan por su nivel de clasificación.

Para tal fin, se pueden apoyar en soluciones tecnológicas de cifrado para la información en medio digital. La información física, no se debe dejar abandonada en impresoras, en el puesto de trabajo o un área de circulación alta de personas.

Para el tratamiento de información tipo verbal, se debe tener reserva y solo comentarla en áreas o zonas seguras dentro de la entidad.

5.21 Política Gestión de Contraseñas

Para controlar el acceso de la información y restringirla sólo al personal autorizado conforme el perfil de acceso, el Oficial de Seguridad de la Información, define 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 **MINMINAS** 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.

Para la gestión de contraseñas, se define:

- Asignar el uso de contraseñas individuales por cada parte interesada, para determinar responsabilidades por persona.
- Queda prohibido la asignación de contraseñas de acceso compartidas y el uso de cuentas genéricas en los sistemas de información.
- Se permite que los usuarios seleccionen y cambien sus propias contraseñas.
- Las contraseñas deben ser complejas y no deben ser palabras comunes ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
- Se debe cambiar la contraseña obligatoriamente la primera vez que el usuario ingrese al sistema de información.
- Se debe cambiar obligatoriamente la contraseña cada 60 días o cuando lo establezca el Oficial de Seguridad de la Información, por temas de incidentes de seguridad.
- Se debe mantener un registro de las últimas 6 contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
- Se debe evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
- Las contraseñas no deben registrarse en papel, archivos digitales o dispositivos móviles, a menos que se puedan almacenar de forma segura y el método de almacenamiento seguro este aprobado por el Oficial de Seguridad de la Información.
- Se requiere modificar todas las contraseñas predeterminadas que por defecto vienen asignadas por los fabricantes en el software y el hardware nuevo y existente

(por ejemplo: contraseñas en impresoras, firewall, router, switch, apache, entre otros).

5.22 Política Seguridad Ambiental

El **MINMINAS** 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 disminuir 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 consideras áreas o zonas seguras.

Los ingresos y egresos de todo el personal a las instalaciones físicas del **MINMINAS** deben ser registrados sin excepción, es decir, que las partes interesadas, deben cumplir completamente con los controles físicos implantados en la entidad.

Todas las partes interesadas del **MINMINAS** deben portar el carnet siempre en un lugar visible, al igual que los visitantes, mientras se encuentren en las instalaciones de la entidad. En caso de pérdida del carnet o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible al Grupo de Servicios Administrativos.

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.

Así mismo, se debe registrar el ingreso de los visitantes a las áreas seguras en una bitácora física ubicada en la entrada de estos lugares de forma visible o mediante un software de control de visitantes.

Todos las partes interesadas y visitantes deben portar una cinta y carnet visible mientras permanezcan en las instalaciones del **MINMINAS**, sin excepción.

Las personas que se detecten sin el carnet, se tratará como un incidente de seguridad de la información y se hará su respectivo llamado de atención por el incumplimiento de las políticas establecidas por el **MINMINAS**.

5.23 Política de seguridad física

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

El **MINMINAS** 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.

Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación como una tarjeta o una sala de recepción atendida por personas. La implementación y la fortaleza de cada barrera estarán definidas por el responsable del área, con el asesoramiento del Oficial de Seguridad de la Información y empresas externas especializadas, de acuerdo a los resultados de la evaluación de riesgos físicos que se debe realizar cada año.

5.23.1 Protección contra amenazas internas y externas

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

En la selección de los mecanismos de protección lógica, se deben tener en cuenta amenazas como la ingeniería social, el robo de información, destrucción de información, saboteo a sistemas de información, suplantación de identidad, estafas digitales, código malicioso, denegación de servicio, ataques a los servicios de red, alteración de la página web del **MINMINAS**, suplantación de cuentas de correo, ataques de correo no deseado (SPAM), archivos manipulados con código para explotación, herramientas de acceso remoto no autorizado, entre otros, por lo cual el análisis de riesgos de seguridad de la información y la implementación de controles adecuados pueden reducir la posibilidad de las mismas.

5.23.2 Trabajo en áreas seguras

La información sobre la naturaleza, localización y disposición de los sistemas de procesamiento y almacenamiento de información del **MINMINAS**, 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.

Se debe diseñar y aplicar protección física y pautas para trabajar en las áreas definidas como seguras en el **MINMINAS**, como por ejemplo el Centro de Cómputo del piso 4, el área de gestión documental, el área de archivo de cada dependencia, el área de equipos de CCTV del primer (1) piso, las oficinas con acceso restringido, como por ejemplo: el Despacho del Ministro, el cuarto de la planta eléctrica y UPS, el Archivo Central, el almacén del primer (1) piso, la ventanilla de atención al ciudadano, terraza del edificio (antenas de comunicación), entre otros, como por hacer alusión a los más importantes.

Esas zonas o áreas seguras deben estar demarcadas y con el aviso de acceso restringido, como recomendación.

5.24 Política Acciones Correctivas

Se integra el SGSI al sistema de gestión de calidad ISO 9001:2008 existente en la Entidad, para la gestión de las directrices para eliminar la causa de no conformidades asociadas con los requisitos de la política de seguridad de la información del **MINMINAS**, para identificar, registrar, controlar, desarrollar, implementar y realizar seguimiento a las acciones correctivas necesarias para evitar que se repita la no conformidad, con el apoyo del Oficial de Seguridad de la Información de la entidad.

De acuerdo a la correspondencia y a los vínculos técnicos entre las normas ISO 9001:2008 e ISO 27001:20013, se utiliza el procedimiento de mejora continua AG-P-04 del **MINMINAS** que se encuentra aprobado y publicado en el aplicativo web SIGME.

Las acciones correctivas deben ser puestas en conocimiento de la Mesa de Trabajo de Seguridad y Privacidad de la Información. La Oficina de Control Interno puede hacer el seguimiento al cumplimiento de las mismas. Esto es para conciliar con la Oficina de Planeación, las acciones correctivas que se pretenden adoptar.

GLOSARIO

Activo de información: Cualquier recurso de valor para el MINMINAS, representado en una persona, proceso o tecnología aplicada, de relevancia e importancia que le permiten cumplir con su rol misional, funcional y operacional.

Alta Dirección del Ministerio de Minas y Energía: Se refiere al staff del Ministerio de Minas y Energía, conformado por el Ministro, Viceministros y Secretario General.

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.

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 **MINMINAS**.

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 le correo, cargo, profesión, entidad a la que pertenece, dirección, teléfonos (fijo y móvil), ciudad y país, entre otros.

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 des-configuraciones 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. [Fuente: Wikipedia].

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.

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 **MINMINAS**.

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.

MINMINAS: Abreviación para definir de manera corta al Ministerio de Minas y Energía.

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.

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. [Fuente: Wikipedia].

Partes interesadas: En el presente contexto, se refiere a dos actores: **a)** El **MINMINAS**, 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 **MINMINAS**, stakeholders.

Proveedores críticos: Son aquellas entidades (personas jurídicas) o personas naturales que bajo cualquier modalidad de contratación se encuentran vinculadas con el **MINMINAS**, 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.

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 **MINMINAS**.

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.

Terceros o proveedores: Es toda persona, proveedor, que está implicada directamente con vínculo contractual en el **MINMINAS**, 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.