REPÚBLICA DE COLOMBIA

Libertad y Orden

UNIDAD DE PLANEACIÓN MINERO ENERGÉTICA - UPME

RESOLUCIÓN No. 000340 de 2021

13-10-2021

Radicado ORFEO: 20211140003405

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información en la Unidad de Planeación Minero Energética - UPME"

EL DIRECTOR GENERAL DE LA UNIDAD DE PLANEACIÓN MINERO ENERGÉTICA - UPME

En ejercicio de sus facultades legales, y especialmente las conferidas por el artículo 9 del Decreto 1258 2013, y

C O N S I D E R A N D O:

Que el artículo 209 de la Constitución Política de la República de Colombia establece que "*La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones*".

Que conforme lo dispuesto el numeral 8 del artículo 2 de la Ley 1341 de 2009 y en seguimiento del principio de 'masificación del gobierno en línea', hoy Gobierno Digital, las entidades públicas 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 para consolidar la prestación de un servicio eficiente a los ciudadanos.

Que el artículo 2.2.22.2.1 del Decreto 1083 de 2015, establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran la política número 11. Gobierno Digital, antes Gobierno en Línea, y la política número 12 de Seguridad Digital.

Que el Decreto 1078 de 2015 "*Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones*", dispone en el artículo 2.2.9.1.2.1 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 el Documento CONPES 3854 de 2016 establece la *Política Nacional de Seguridad Digital en la República de Colombia*, fortaleciendo las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital y se generarán mecanismos permanentes para impulsar la cooperación, colaboración y

asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

Que el artículo 1 del Decreto 1008 de 2018, "*por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones*", determinó los principios y los elementos de la Política de Gobierno Digital

Que conforme al principio de Seguridad de la Información de la Política de Gobierno Digital, se deben crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado y de los servicios que prestan al ciudadano.

Que el Documento CONPES 3995 de 2020 formula la *Política Nacional de Confianza y Seguridad Digital en la República de Colombia*, estableciendo medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital, fortaleciendo las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país; actualizando el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y finalmente, se analizará la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías.

Que en seguimiento de lo anterior, la Unidad de Planeación Minero Energética - UPME diseñó la Política de Seguridad y Privacidad de la Información, la cual contiene los lineamientos y medidas de seguridad que deberán ser atendidos por sus colaboradores, proveedores y partes interesadas que tengan acceso a la información, para la protección física o digital de los activos de información de la entidad.

Que la implementación de esta política busca poner en marcha las medidas técnicas humanas y administrativas necesarias para prevenir la adulteración, pérdida, consulta, uso y/o acceso no autorizado de la información.

Que en sesión celebrada el día 11 de junio de 2021 por parte del Comité Institucional de Gestión y Desempeño de la UPME (Comité No.7), fue sometida a consideración y se aprobó recomendar a la Dirección General adoptar la actualización de la Política de Seguridad y Privacidad de la Información de la entidad.

Que en seguimiento de lo dispuesto por la Resolución UPME 087 de 2021 "*Por la cual se reglamenta la elaboración y la publicación de los proyectos de actos administrativos de carácter general y abstracto emitidos por la UPME*", el proyecto de resolución junto con la memoria justificativa fueron publicados en el sitio web de la entidad para recibir comentarios y observaciones de los ciudadanos por un periodo de quince (15) días calendario entre el 21 de septiembre y el 6 de octubre de 2021, conforme a lo dispuesto mediante la Circular Externa No. 046 de 2021.

Que una vez concluido el periodo de consulta, no se recibieron comentarios ni observaciones al proyecto normativo, por lo cual no se hace necesario la elaboración del informe global de observaciones y respuestas.

Que en mérito de lo expuesto,

R E S U E L V E:

ARTÍCULO 1: ADOPCIÓN. Adoptar la *"Política de Seguridad y Privacidad de la Información"* de la Unidad de Planeación Minero Energética – UPME, la cual hace parte integral del presente acto administrativo.

ARTÍCULO 2: COMUNICACIÓN. Comunicar la *"Política de Seguridad y Privacidad de la Información"* a todos los colaboradores (Funcionarios y Contratistas) de la Unidad de Planeación Minero Energética – UPME, así como a los grupos de interés y ciudadanía en general, mediante su publicación en la página web de la entidad.

ARTÍCULO 3: DECISIÓN. Las decisiones y la gestión de los temas relacionados con la *"Política de Seguridad y Privacidad de la Información"* serán discutidos en el Comité Institucional de Gestión y Desempeño de la UPME, con el apoyo del Oficial de Seguridad de la entidad y siguiendo los lineamientos que en esta materia existan en la administración pública colombiana.

ARTÍCULO 4: ACTUALIZACIÓN. La *"Política de Seguridad y Privacidad de la Información"* será revisada y actualizada, de acuerdo con las necesidades o cambios en la estrategia institucional y/o de los lineamientos gubernamentales, mediante acto administrativo.

ARTÍCULO 5: RESPONSABLES. El Oficial de Seguridad de la UPME será el responsable de liderar y coordinar la implementación de la *"Política de Seguridad y Privacidad de la Información"*, con la participación activa de las dependencias de la entidad.

ARTÍCULO 6: VIGENCIA. La presente Resolución rige a partir de la fecha de su publicación en el Diario Oficial y deroga todas las disposiciones anteriores que le sean contrarias.

COMUNÍQUESE Y CÚMPLASE,

Dada en Bogotá, D.C., a **13-10-2021**

CHRISTIAN JARAMILLO HERRERA
Director General

Elaboró: Carlos Humberto Parra- Luis Hurtado- Elkin Rojas- José Emilio Ramírez – Jannluck Canosa Cantor
Revisó: Ligia Galvis Amaya – Jimena Hernández
Aprobó: Diana Helen Navarro Bonet

Política de Seguridad y Privacidad de la Información

1. INTRODUCCIÓN.

El presente documento contiene las Políticas y Normas de Seguridad de la Información que servirán de guía para los funcionarios de la Unidad de Planeación Minero Energética (UPME) desde la Alta Dirección, hasta todos los niveles jerárquicos de la entidad, sobre la importancia que tiene la seguridad de la Información en la Entidad.

Adicionalmente, se define la metodología que contiene los parámetros utilizados en el diseño e implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la Norma ISO 27001:2013 y la resolución No. 00500 del 10 de marzo de 2021 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones, donde se describe la gestión del riesgo de información de la entidad y los objetivos de la seguridad de la información como es la confidencialidad, integridad y disponibilidad, para de esta manera y a través de los controles que propone la norma llegar a establecer el plan de tratamiento que se va a dar a los riesgos encontrados y el nivel de aceptación de riesgo que está dispuesto a asumir la entidad.

Además de lo anterior, se enuncian los procedimientos relacionados con las políticas y normas de seguridad establecidas anteriormente.

El normograma correspondiente a todos aquellos aspectos normativos y leyes aplicables a la Unidad de Planeación Minero Energética (UPME) y que tengan relación con la seguridad de la información, aspectos que se tienen en cuenta en este documento se presentan en el documento anexo “Normograma de Política de Seguridad y Privacidad de la Información”.

1.1. Objetivo.

El objetivo principal de este documento es describir las políticas y normas de seguridad de la información diseñadas para la Unidad de Planeación Minero Energética (UPME), así como la relación de los procedimientos asociados a las políticas establecidas que permitan asegurar la confidencialidad, integridad y disponibilidad de la información.

1.2. Alcance

Este documento provee las políticas de seguridad establecidas bajo el estándar NTC ISO 27001:2013 y los aspectos normativos vigentes a que haya lugar, cubren las responsabilidades y deberes de los colaboradores de la entidad en el Sistema de Gestión de Seguridad de la Información SGSI.

2. TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN.

Los siguientes términos y definiciones están basados en la Norma ISO 27001: 2013 y son aplicables a la Unidad de Planeación Minero Energética (UPME) y al Sistema de Seguridad de la Información de la misma:

2.1. Términos y definiciones de la Norma ISO 27001:2013

Para una mejor comprensión del presente Manual, se toman como referencia los siguientes términos y definiciones establecidos en la Norma ISO 27001:2013:

- **Aceptación de riesgo:** Decisión de asumir un riesgo.
- **Activo:** Cualquier cosa que tiene valor para la organización.
- **Análisis de Riesgo:** Uso sistemático de la información para identificar fuentes y para estimar el riesgo (Guía ISO/IEC 73:2002).
- **Adaptabilidad:** Define los eventos y bajo qué criterios un sistema debe poder ser monitoreado y revisado para su control posterior.
- **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidad.
- **Confiabilidad de la Información:** Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Declaración de aplicabilidad:** Documento que describe los objetivos de control y los controles pertinentes y aplicables para el mismo.
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad.
- **Evaluación del riesgo:** Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.
- **Evento de seguridad de la información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.
- **Incidente de seguridad de la información:** Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad d la información.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

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

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

- **Responsable de Seguridad Informática:** En la Unidad de Planeación Minero Energética (UPME) el comité institucional de gestión y desempeño será el grupo encargado de realizar el seguimiento y monitoreo al Sistema de Gestión de la Seguridad de la Información (SGSI).

- **Riesgo: "**El efecto de la incertidumbre sobre los objetivos". (Icontec, 2011, Pág.4)

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

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

- **Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad. [NTC-ISO/IEC 17799:2006]

- **Sistema de gestión de la seguridad de la información SGSI:** Parte del sistema de gestión global, basado en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

- **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales que se realicen en la Unidad de Planeación Minero Energética (UPME).

- **Tecnología de la Información:** Se refiere al hardware y software operado por la organización por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Unidad de Planeación Minero Energética (UPME).

- **Tratamiento del riesgo:** Proceso de selección e implementación de acciones de mejora que permita gestionar el riesgo.

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

2.2. Términos y definiciones utilizados en las matrices de inventario de activos de información como parte del SGSI.

Para lograr comprender todos los términos y parámetros utilizados en las Matrices de Activos de Información del Sistema de Gestión de la Información bajo la Norma ISO 27001:2013 se tomaron como referencia los siguientes términos:

- **N° de activo:** Codificación de cada activo de información.
- **Nombre del activo:** Cualquier tipo de información soportada por un medio físico o tecnológico que tenga valor para la organización.
- **Dueño del riesgo sobre el activo:** Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- **Responsables del Activo:** Personas responsables del activo de información en el proceso.
- **Clasificación de activos:** Tipos de activos de información presentes en cada proceso.
- **Nivel de criticidad:** Nivel crítico del activo de información en el proceso.
- **Impacto en los activos de información por la modificación de los mismos**
  - ✓ **Impacto Leve:** Modificación leve del activo de información.
  - ✓ **Impacto Importante:** Modificación importante del activo de información.
  - ✓ **Impacto Grave:** Modificación grave del activo de información.
- **N° de riesgo:** Codificación de cada riesgo.
- **Riesgo:** Efecto de la incertidumbre sobre el cumplimiento de los objetivos.
- **Probabilidad de ocurrencia:** Posibilidad de que se presente una situación específica.
- **Impacto:** Nivel de afectación en el activo de información que se genera al existir el riesgo.
- **Nivel de riesgo:** Da el resultado en donde se ubica el riesgo por cada activo de información.
- **Clasificación:** Da el resultado en donde se ubica el riesgo por cada activo de información.
- **Nivel de Criticidad:** Nivel crítico del activo de información.

2.3. Definición de riesgo en la seguridad de la información.

De acuerdo a la norma técnica (ISO/IEC 27000) riesgo es la “posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias”.

De igual manera, el objetivo general de la norma es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información en la Unidad de Planeación Minero Energética (UPME).

2.4. Incidentes de la seguridad de la información.

Según la norma ISO 27001:2013 un incidente de seguridad de la información está definido como “un evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen la probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información” (ISO27001 Icontec, 2013), por lo cual se establecen los siguientes incidentes que pueden llegar a suceder dentro de la Unidad de Planeación Minero Energética (UPME):

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

2.5. Eventos.

Según la NTC ISO 27001:2013, se define un evento de seguridad de la información como “la presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.” (ISO 27001:2013, ICONTEC, Pág. 11, 2013); por lo tanto, dentro de los eventos de seguridad de la información que se pueden llegar a presentar dentro de la Unidad de Planeación Minero Energética (UPME) se encuentran los siguientes:

Evento	*Descripción*
Fraude Interno	Está asociado a la intención por parte de un funcionario de la organización de obtener información con fines ajenos a su labor, incumpliendo normas y leyes de la Unidad de Planeación Minero Energética (UPME).

Fraude Externo	Son actos realizados por personas externas a la organización, que buscan apropiarse indebidamente de la información, por medio de acceso no autorizado, alterando o vulnerando el procesamiento de la información en la Unidad de Planeación Minero Energética (UPME).
Clientes	Según el Anexo A.9.2.2. de la norma ISO 27001:2013 "Se debe implementar el suministro de acceso formal de usuarios para asignar o revocar los accesos para todo tipo de usuario"
Fallas Tecnológicas	Pérdida de información asociada a fallas tecnológicas presentadas en el procesamiento de la información que vulneran la confidencialidad, integridad y disponibilidad de la misma.
Ejecución y administración de procesos	Pérdida de información asociada a errores de administración y ejecución de procesos en la Unidad de Planeación Minero Energética (UPME).

Tabla 2: Eventos asociados al SGSI
Fuente: Anexo A de la norma ISO 27001:2013.

3. ALCANCE, POLÍTICA Y OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

3.1. Alcance del Sistema de Gestión de Seguridad de la Información - SGSI

En el contexto de la UPME, el alcance de este SGSI – Sistema de Gestión de Seguridad de la Información en UPME, incluye los 3 procesos estratégicos, 8 procesos misionales, 8 procesos de apoyo y 2 procesos de evaluación y control, de acuerdo con el mapa de procesos y los requisitos de las partes interesadas, así:

Estratégicos	DIRECCCION ESTRATEGICO
	COMUNICACIÓN ESTRATEGICA
	INFORMACION SECTORIAL
Misionales	DEMANDA
	PLANEACION INTEGRAL MINERIA
	PLANEACION INTEGRAL HIDROCARBUROS
	PLANEACION INTEGRAL ENERGIA ELECTRICA
	PROYECTOS DE FONDOS
	GESTION CONVOCATORIAS
	DIVULGACION MINERO ENERGETICA

	GESTION DE CONCEPTOS TECNICOS
Apoyo	GESTION TALENTO HUMANO
	GESTION FINANCIERA
	GESTION DOCUMENTAL
	GESTION SERVICIOS ADMINISTRATIVOS
	GESTION CONTRACTUAL
	PARTICIPACION Y SERVICIO AL CIUDADANO
	GESTION JURIDICA
	GESTION TICS
Evaluación y control	EVALUACION Y CONTROL
	MEJORAMIENTO CONTINUO

Todos estos procesos tienen diferentes procedimientos asociados, los cuales están incluidos en cada proceso descrito.

3.2. Política de seguridad de la información.

La Unidad de Planeación Minero Energética – UPME, es una entidad adscrita al Ministerio de Minas y Energía, la cual tiene como función esencial la planeación de manera integral el desarrollo minero energético, apoyando la formulación de política pública y coordinar la información sectorial con los agentes y partes interesadas.

La entidad consciente de la importancia que representa la seguridad de la información ha decido implantar el SGSI y suscribe la presente política.

La Unidad de Planeación Minero Energética -UPME, en lo que se refiere a la planeación en forma integral, indicativa, permanente y coordinada con los agentes del sector minero energético propende por generar mayor confianza entre todas las partes interesadas; por ende ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI), con el apoyo de la alta dirección, orientado a gestionar los riesgos de seguridad de la información entendida como la preservación de la confidencialidad, la integridad y la disponibilidad, así como propender por el cumplimiento de los objetivos definidos para el SGSI, cumplir los requisitos legales aplicables y asegurar el mejoramiento continuo del SGSI en la UPME.

3.3. Objetivos de seguridad de la información

- Administrar la seguridad de la información en la UPME y establecer un marco gerencial para iniciar y controlar su implementación y eficacia, así como para la distribución de funciones y responsabilidades.
- Fomentar la cultura de cooperación con autoridades y entes especializados para la obtención de asesoría en materia de seguridad de la información.
- Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceras partes a la información de la UPME.
- Asegurar la preservación de la integridad, confidencialidad y disponibilidad de la información establecidos en los procesos incluidos en el alcance del SGSI de la UPME.

- Gestionar los riesgos de seguridad de la información a los que se encuentra expuesta la información, identificados en el marco del SGSI.
- Generar cultura sobre la seguridad de la información a todas las partes interesadas en el contexto de la UPME en cuanto a los procesos relacionados con la recepción, tratamiento, aplicación de modelos específicos de la industria, almacenamiento, explotación y divulgación de la información en la UPME.
- Brindar las herramientas necesarias para el desarrollo, maduración y mejoramiento continuo del sistema de gestión de seguridad de la información (SGSI) de la UPME para los procesos relacionados en el alcance de este sistema.

4. METODOLOGÍA PARA EL DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) DE LA UNIDAD DE PLANEACIÓN MINERO ENERGÉTICA (UPME).

Teniendo en cuenta lo establecido en la NTC ISO 27001:2013, el diseño e implementación del Sistema de Gestión de Seguridad de la Información está integrado por las siguientes fases:

- Definición del alcance y los objetivos del SGSI partiendo de los requerimientos y necesidades establecidos por la entidad.
- Definición de la Política de Seguridad y privacidad de la Información que establece un parámetro a seguir en la seguridad de la información y se alinea con el contexto estratégico de la entidad.
- Definición del enfoque de la Unidad de Planeación Minero Energética (UPME) para la valoración del riesgo mediante el establecimiento de la metodología que cumpla con los requisitos del SGSI de la entidad y el desarrollo de criterios de aceptación de riesgo que está dispuesta a asumir.
- Análisis del riesgo de la información mediante la identificación de activos, amenazas, vulnerabilidades e impactos relacionados a estos.
- Valoración del riesgo mediante el establecimiento del impacto, la probabilidad de ocurrencia, estimación de niveles de riesgos y de aceptación de estos.
- Identificación del plan de tratamiento para mitigar los riesgos.
- Seguimiento, medición y análisis del Sistema de Gestión de la Seguridad de la Información.
- Auditorías internas
- Revisión por parte de la Alta dirección.
- Establecimiento de planes de mejoramiento continuo del SGSI.

4.1. Identificación de los roles, responsabilidades y autoridades en la organización.

Lineamiento: Articular con las áreas o dependencias de la Entidad, los roles y responsabilidades necesarios para la adopción del MSPI, el monitoreo del desempeño y el reporte y seguimiento ante el comité institucional de gestión y desempeño, para que sean aprobados y comunicados dentro de la UPME.
Se debe delegar a un responsable de la seguridad y privacidad de la información y el equipo humano necesario para coordinar la implementación del MSPI.

La Alta Dirección de la Unidad de Planeación Minero Energética (UPME), está comprometida con el Sistema de Gestión de Seguridad de la Información, por lo tanto, propenderá por:

- El establecimiento de objetivos dentro del Sistema de Gestión de Seguridad de la Información, que sean coherentes con el objetivo general de la entidad.
- El control por parte de la dirección del Sistema de Gestión de Seguridad de la Información se realizará a través de revisiones periódicas, las cuales serán planificadas, cumpliendo con los requerimientos del SGSI y de la entidad.
- Establecimiento y aprobación de la política de Seguridad y privacidad de la Información, la cual deberá ser publicada y divulgada a toda la entidad.
- Implementación de acciones tanto preventivas como correctivas que permitan a la Unidad de Planeación Minero Energética (UPME) la mitigación de los riesgos potenciales.
- Revisión y actualización de la política de seguridad de la información de manera periódica.

4.2. Identificación de Riesgos de Seguridad de la Información en la UPME

Dentro de los requisitos establecidos por la norma ISO27001:2013, se debe realizar una identificación de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

En la UPME, está alineado con el anexo 1 del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, cuyo objetivo en esta etapa es identificar los riesgos que estén o no bajo el control de la entidad, para ello se debe tener en cuenta el contexto estratégico en el que opera la Unidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Se tienen las siguientes fases:

- Análisis de objetivos estratégicos y de los procesos.
- Identificación de los puntos de riesgo.
- Identificación de áreas de impacto.

- Identificación de áreas de factores de riesgo.
- Descripción del riesgo.

De acuerdo con lo sugerido en dicho modelo y otras prácticas de seguridad de la información:

a) Se identifican los activos de información dentro de los procesos del alcance del SGSI, se clasifican y se determina su criticidad.
b) Se establecen los responsables y dueños de los riesgos de cada activo de información que se encuentran asociados a estos activos.
c) Teniendo en cuenta el conocimiento de las actividades de la entidad por parte de los funcionarios y el comportamiento histórico de los procesos, se identifican los riesgos de seguridad de la información a través de un entendimiento previo de los procesos. Los riesgos se identifican de acuerdo con las posibles amenazas y las vulnerabilidades a las que pueda estar expuesto el activo, afectando en alguna medida la confidencialidad, integridad o disponibilidad de la información.

4.3. Valoración de los riesgos de seguridad de la información en la UPME.

La Unidad de Planeación Minero Energética (UPME) utiliza una metodología para valorar los riesgos de Seguridad de la Información, basada en la calificación del impacto y la probabilidad de ocurrencia, para obtener los niveles de riesgo. Dicha metodología abarca los siguientes aspectos:

a) Se determina la probabilidad de ocurrencia para cada riesgo teniendo en cuenta los siguientes criterios de valoración:

Valoración	*Valor Asignado*	*Factibilidad*	*Frecuencia*
Raro	1	Evento que puede ocurrir solo en circunstancias excepcionales.	No se han presentado en los últimos 5 años
Improbable	2	El evento puede ocurrir en algún momento.	Al menos una (1) vez se ha presentado en los últimos 5 años
Posible	3	El evento podría ocurrir en algún momento.	Al menos una (1) vez se ha presentado en los últimos 2 años
Probable	4	El evento que probablemente ocurrirá en la mayoría de las circunstancias.	Al menos una (1) vez se ha presentado en el último año
Casi Seguro	5	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de (1) vez se ha presentado en el último año

Tabla 7: Valoración de la probabilidad de ocurrencia
Fuente: UPME

b) Se establece la valoración del impacto generado por cada riesgo teniendo en cuenta los siguientes parámetros de evaluación:

Valoración	*Valor Asignado*	*Criterio*
Insignificante	1	Afectación muy leve de la confidencialidad, integridad y disponibilidad de la información crítica de la Unidad de Planeación Minero Energética (UPME).
Menor	2	Afectación leve de la confidencialidad, integridad y disponibilidad de la información crítica de la Unidad de Planeación Minero Energética (UPME).
Moderado	3	Afectación Moderada de la confidencialidad, integridad y disponibilidad de la información crítica de la Unidad de Planeación Minero Energética (UPME).
Mayor	4	Afectación grave de la confidencialidad, integridad y disponibilidad de la información crítica de la Unidad de Planeación Minero Energética (UPME).
Catastrófico	5	Afectación muy grave de la confidencialidad, integridad y disponibilidad de la información crítica de la Unidad de Planeación Minero Energética (UPME).

Tabla 8: Valoración del Impacto
Fuente: UPME

Se establecieron los niveles de riesgos teniendo una clasificación propia para la Unidad de Planeación Minero Energética (UPME) basada en la probabilidad de ocurrencia y el impacto evaluado con anterioridad:

Tipo de riesgo	*Valor Asignado*	*Acción requerida*
Riesgo Extremo	Mayor a 15	Requiere acciones inmediatas para evitar.
Riesgo Alto	Mayor o igual a 6 y menor de 15	Requiere de acciones rápidas por parte de la Alta Dirección para disminuir el riesgo.
Riesgo Medio	Mayor o igual 4 y menor de 6.	Requiere de medidas, prontas y adecuadas que permitan disminuir el riesgo a niveles inferiores del actual.
Riesgo Bajo	Menor a 4	La entidad podría optar por aceptar el riesgo sin tomar otras acciones adicionales a los controles ya establecidos.

Tabla 9: Niveles de Riesgos

4.4. Evaluación de los controles establecidos para la mitigación de los riesgos.

La Evaluación de los controles se realiza cuando se ha establecido el riesgo inherente en cada activo de información, y el impacto y probabilidad de ocurrencia de cada uno de los riesgos establecidos. La evaluación de controles se realiza de la siguiente manera:

a. Identificación de los controles relacionados a cada uno de los riesgos establecidos. Es necesario determinar si el control existe y de no ser así se deja el registro.

b. Si los controles existen, se realiza la calificación de cada uno teniendo como criterio las cualidades y características. Se tienen como cualidades de los controles las siguientes:

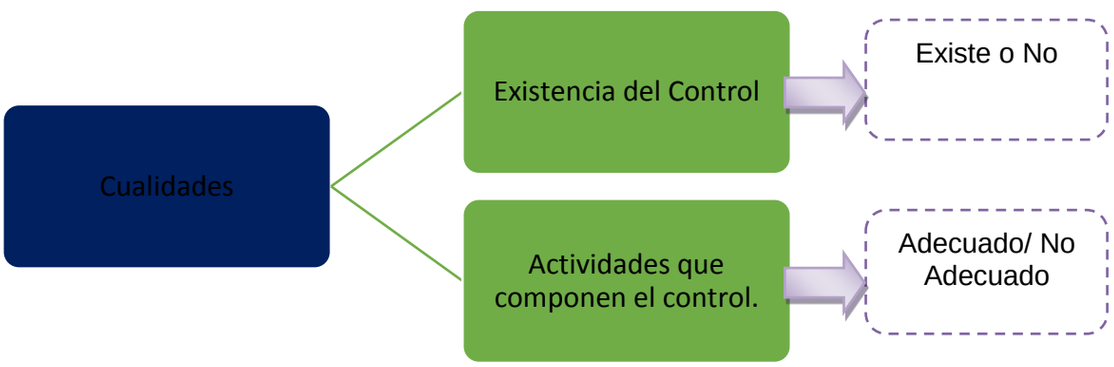

Figura 8: Cualidades de los controles

c. Las características se resumen en lo siguiente:

CARACTERÍSTICAS	*DESCRIPCION*
Categoría del Control	Establece si es control es operativo, táctico o estratégico.
Naturaleza del Control	Determina si el control es manual, mixto o automático
Funcionalidad de la Naturaleza	Significa que la naturaleza del control como tal resulta adecuada o no dentro de la actividad del mismo control
Documentación	Establece si el control está documentado (si) / no está documentado (no).

Periodicidad de ejecución	Periodo de tiempo en que se realiza o se ejecuta el control: Múltiples veces al día, diario, Mensual, semestral, anual y cada vez que se presenta.
Complejidad	Establece el grado de complejidad de la ejecución del control (complejo no complejo).
Funcionalidad de la complejidad	Si el control es: adecuado o no adecuado
Responsabilidad	Determina si la responsabilidad esta: definida o no definida
Cargo	Nombre del cargo que ejecuta el control.
Tipo de control	Control: detectivo, preventivo o correctivo.
Importancia sobre la mitigación del riesgo	Percepción del dueño del riesgo del riesgo del activo: establece si este control es relevante para mitigar el riesgo - importante o no importante.
Disminuye la probabilidad	Percepción del dueño del riesgo del activo: establece si el control llega a disminuir la probabilidad de ocurrencia del riesgo - SI/ NO.
Disminuye el impacto	Percepción del dueño: establece si el control llega a disminuir el impacto del riesgo- SI/ NO.
Observaciones	Comentarios a los que hubiere lugar.

Tabla 10: Características de los controles

d. Las cualidades tienen una ponderación del 20% dentro del total de la valoración de los controles y las características el 80%. A su vez cada variable dentro de las cualidades y las características tienen una ponderación dependiendo el grado de importancia como se muestra a continuación:

CUALIDADES	
20%	¿El control Existe?
	Actividades que componen el control
CARACTERÍSTICAS	
80%	Naturaleza del Control
	Funcionalidad de la Naturaleza
	Documentación
	Complejidad
	Funcionalidad de la complejidad
	Responsabilidad
	Tipo de control
	Importancia sobre la mitigación del riesgo

	Disminuye la probabilidad
	Disminuye el impacto

Tabla 11: Criterios para la evaluación de los controles

e. Los valores de cada grupo de variables se suman y da un valor para cada control.

f. Si se establece más de un control para el riesgo, se realiza el mismo procedimiento de calificación por cada uno de los controles y luego se realiza una ponderación de la evaluación dependiendo el número de controles establecido para obtener el nivel de control.

g. El nivel de control se compara con un valor asociado al apetito de riesgo. Los niveles de control podrán tener o encajar en los siguientes rangos:

- "Controles no Efectivos"
- "Poco Efectivo"
- "Efectivo"
- "Muy efectivo".

h. Finalmente, la calificación del control determina el desplazamiento o no del riesgo en sus niveles de impacto y probabilidad, dependiendo, entre otros aspectos, de si los controles disminuyen o no los niveles de probabilidad e impacto obtenidos en el riesgo inherente.

El desplazamiento de los riesgos tiene en cuenta la matriz de referencia (Ver Tabla 12) y el número de controles, de forma semicuantitativa. Contando con el hecho que los controles disminuyan alguna de las dos variables probabilidad o impacto, ayuda a determinar el número de unidades para dicho desplazamiento y por último la efectividad de los mismos (promediada). Podría haber un máximo desplazamiento de 4 unidades, por si el valor del impacto (Catastrófico) y/o probabilidad (Casi Seguro), fuere 5.

Por ejemplo, un riesgo inherente cuyo valor en probabilidad es 3 e impacto es 2, podría tener tres controles asociados, donde dos de ellos disminuye los niveles de probabilidad, pero ninguno disminuye el nivel del impacto. Si dos de los tres controles, según la evaluación, disminuye probabilidad, significa que el promedio es 0,7 (2 dividido en 3 controles) para valor inherente 3, el desplazamiento según matriz sería de dos unidades, es decir su nuevo valor de probabilidad sería 1 y el nuevo nivel de riesgo que era (3,2), bajaría a un nivel de riesgo (1,2).

	Valor Actual				
Promedio	**1**	**2**	**3**	**4**	**5**
1	0	1	2	3	4
0,9	0	1	2	3	4
0,8	0	1	2	3	4
0,7	0	1	2	2	3

0,6	0	1	1	2	3
0,5	0	1	1	1	2
0,4	0	0	1	1	2
0,3	0	0	1	1	1
0,2	0	0	0	1	1
0,1	0	0	0	0	1

Tabla 12: Unidades de desplazamiento del riesgo tras la evaluación de controles

4.5. Establecer un plan de tratamiento de cada uno de los riesgos de información de la Unidad de Planeación Minero Energética (UPME).

Con base en el resultado del análisis de riesgo y con el fin de gestionar el riesgo residual se proponen acciones de mejora las cuales pueden estar en marcha por medio de planes de acción o de tratamiento, con la finalidad que la información siempre conserve las características de confidencialidad, integridad y disponibilidad de la misma.

Cada plan de acción se define y desarrolla en particular dependiendo de:

a) Si se encuentra en una zona de aceptación o apetito de riesgo.

b) Si es susceptible de ser tratado a través de la implantación de un nuevo control o fortaleciendo los ya existentes.

c) Si la decisión es aceptarlo, independiente de donde se encuentre ubicado y la afectación que pueda tener para Confidencialidad, Integridad y Disponibilidad de la información.

d) Si se decide ignorar, determinar la reiniciación del análisis.

e) Si la decisión es transferir, realizar los análisis de costo beneficio correspondiente.

5. SEGUIMIENTO, MEDICION, ANALISIS Y EVALUACION DEL SGSI EN UPME

Según la norma técnica colombiana NTC: ISO 27001: 2013, la Unidad de Planeación Minero Energética (UPME) debe “evaluar el desempeño de la seguridad de la información y la eficiencia del SGSI”, por medio de:[1]

5.1. Auditorías internas.

La Unidad de Planeación Minero Energética (UPME) programa y ejecuta auditorías internas con fechas planificadas, tal como lo establece la norma ISO 27001:2013.

[1] Tomado del estándar para seguridad de la información ISO 27001:2013

5.2. Revisión por parte de la alta dirección.

Según la norma ISO 27001:2013, la Alta Dirección propende por realizar revisiones y el respectivo seguimiento al SGSI en las fechas planificadas.

6. MEJORAMIENTO CONTINUO DEL SGSI EN UPME

El sistema de Gestión de la Seguridad de la Información tiene como finalidad la generación de acciones que permitan a la entidad tener un proceso de mejoramiento continuo del SGSI, por lo que basados en la norma ISO 27001:2013, se establece que:

a) Cuando existan no conformidades, la Unidad de Planeación Minero Energética (UPME) debe mitigar el impacto de su existencia, tomando acciones para controlarla y prevenirla. Adicionalmente establece y hace frente a las consecuencias propias de la no conformidad que llegó a materializarse.

b) Se definen las acciones para disminuir las causas de las no conformidades así:

- Revisión y evaluación de la no conformidad encontrada.
- Establecimiento de las posibles causas y consecuencias que se generaron de la no conformidad.
- Determinar si existen otras no conformidades similares para establecer acciones preventivas evitando así que estas lleguen a materializarse.
- Emprender acciones detectivas que permitan gestionar el riesgo a tiempo, disminuyendo el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de no conformidades dentro del SGSI.

c) Adicionalmente se lleva un registro documentado del tratamiento realizado a la no conformidad, así como las acciones realizadas para mitigar el impacto de esta y su resultado, para futuras no conformidades.

7. POLÍTICAS.

Creación de políticas

Las políticas de la Unidad de Planeación Minero Energética (UPME) deben ser creadas por la función de seguridad de la información y respaldadas por la Alta Dirección de la entidad con la asesoría de las áreas técnicas responsables de los temas asociados a las mismas.

Aprobación de políticas

Las políticas de la Unidad de Planeación Minero Energética (UPME) deben ser aprobadas por la Alta Dirección con base en las recomendaciones del Comité institucional de gestión y desempeño.

Actualización de políticas

Cualquier requerimiento de modificación de las políticas debe ser dirigido al Comité institucional de gestión y desempeño quien será el encargado de mantener actualizado el modelo de seguridad de la Unidad de Planeación Minero Energética (UPME).

Toda modificación a las políticas debe ser aprobada por la Alta Dirección de la entidad.

Nombre de las políticas

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

Estructura de la política

La estructura de la Política de Seguridad es:

- Título de la Política.
- Definición de la Política.
- Fecha de Vigencia.
- Fecha de Actualización.
- Acciones de despliegue e implementación
- Responsable de implementación.

Reglas de escritura de las políticas

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

7.1. Políticas concernientes a la administración de la Unidad de Planeación Minero Energética (UPME) (PA)

Las siguientes Políticas de Seguridad de la Información son responsabilidad de la Administración de la Unidad de Planeación Minero Energética (UPME) según lo establecido en la NTC ISO/IEC 27001:2013.

7.1.1. Políticas de seguridad de la información.

PA001
Título de la Política: Política de la seguridad de la información - *Ref.: ISO/IEC 27001 CL A.5.1.1*

Definición de la Política: La Unidad de Planeación Minero Energética -UPME, en lo que se refiere a la planeación en forma integral, indicativa, permanente y coordinada con los agentes del sector minero energético propende por generar mayor confianza entre todas las partes interesadas; por ende ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI), con el apoyo de la alta dirección, orientado a gestionar los riesgos de seguridad de la información entendida como la preservación de la confidencialidad, la integridad y la disponibilidad de la información, así como propender por el cumplimiento de los objetivos definidos para el SGSI, cumplir los requisitos legales aplicables y asegurar el mejoramiento continuo del SGSI en la UPME.
Acciones de Despliegue e Implantación: ● Definir las políticas de Seguridad de la Información de la Unidad de Planeación Minero Energética (UPME). ● Aprobar y divulgar en la entidad la política de Seguridad de la Información. ● Seguir procedimiento de revisión y mantenimiento de políticas.
Fecha de Creación: octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información

PA002 **Título de la Política: Revisión de las políticas para la seguridad de la información - *Ref.: ISO/IEC 27001 CL A.5.1.2***
Definición de la Política: Las políticas de seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas, siendo responsabilidad de la Alta Dirección el aprobar los ajustes y cambios pertinentes.
Acciones de Despliegue e Implantación: ● Actualizar las políticas de Seguridad de la Información de la Unidad de Planeación Minero Energética (UPME) con la frecuencia definida o cuando haya lugar a un ajuste significativo. ● Seguir procedimiento de revisión y mantenimiento de políticas
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

7.1.2. Organización de la seguridad de la información - Ref.: ISO/IEC 27001 CL A.6

Con la finalidad de realizar la correcta distribución de roles y responsabilidades, atendiendo a la debida segregación de funciones, se establecen las responsabilidades para las áreas funcionales dentro de la entidad.

PA003

Título de la Política: Organización interna de la seguridad de la información - *Ref.: ISO/IEC 27001 CL. A.6.1*

Definición de la Política: La estructura de seguridad de la información debe estar conformada por los siguientes actores a quienes se les debe definir roles y responsabilidades, según la - *Ref.: ISO/IEC 27001 CL. A.6.1.1:*

- **Comité institucional de gestión y desempeño:** El Comité institucional de gestión y desempeño, integrado por representantes de la Dirección General, la Secretaria General, la Subdirección de Demanda, la Subdirección de Energía Eléctrica, la Subdirección de Hidrocarburos, la Subdirección de Minería, el Jefe de la Oficina de Gestión de la Información y el Jefe de la Oficina de Proyectos de Fondos, destinado a garantizar el apoyo manifiesto de todos a las iniciativas de seguridad. El mismo contará con un Coordinador quien será el Oficial de Seguridad de la entidad.
- **Oficial de seguridad de la información:** Será el responsable por la implementación, operación, mantenimiento y mejoramiento de manera transversal en la entidad del Sistema de Gestión de Seguridad de la Información.

Acciones de Despliegue e Implantación:

- Conformar la estructura para la gestión de la seguridad de la información en la Unidad de Planeación Minero Energética (UPME).
- Definir roles y responsabilidades para la estructura conformada.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PA004

Título de la Política: Contacto con las autoridades - *Ref.: ISO/IEC 27001 CL A.6.1.3*

Definición de la Política: La entidad mantiene contacto con las entidades que representen autoridad en temas de seguridad de la información con el fin de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, se mantendrán contactos con las siguientes entidades especializadas en temas relativos a la seguridad de la Información:

- **Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), y particularmente con:**

FIRST – Forum of Incident Response and Security Teams. (www.first.org)

El Foro de Equipos de Seguridad para Respuesta a Incidentes - FIRST es la primera organización global reconocida en respuesta a incidentes, tanto de manera reactiva como proactiva. FIRST reúne una variedad de equipos de respuesta de incidentes de seguridad informática para las entidades gubernamentales, comerciales y académicas. FIRST busca fomentar la cooperación y coordinación en la prevención de incidentes, estimular la reacción rápida a los incidentes y promover el compartir información entre los miembros y la comunidad.

COLSERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia. (http://www.colcert.gov.co/)
El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT, tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual está enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal es la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional.

CSIRT-Gobierno – Equipo de Respuesta a Incidentes de Seguridad Informática Colombia.
CSIRT-Gobierno es un Equipo de Respuesta frente a Incidencias de Seguridad Informática, el cual está en contacto directo con los centros de seguridad de las entidades gubernamentales del orden nacional y territorial y está en capacidad de coordinar el tratamiento y solución de las solicitudes y denuncias sobre problemas de seguridad informática que sean recibidas.

CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia. (http://www.cert.org.co/)
CSIRT-CCIT es un centro de coordinación de atención a incidentes de seguridad informática colombiano, el cual está en contacto directo con los centros de seguridad de sus empresas afiliadas y está en capacidad de coordinar el tratamiento y solución de las solicitudes y denuncias sobre problemas de seguridad informática que sean recibidas.

En conclusión, el CSIRT-CCIT es un punto de contacto nacional, mediante el cual la comunidad nacional e internacional puede comunicarse con las más grandes empresas proveedoras de Internet en Colombia, con el objetivo de gestionar una pronta y eficiente atención a los incidentes de seguridad informática que involucren redes y/o servicios colombianos.

CCP – Centro Cibernético Policial. (http://www.ccp.gov.co/)
El Centro Cibernético Policial es la dependencia de la Dirección de Investigación Criminal e INTERPOL encargada del desarrollo de estrategias, programas, proyectos y demás actividades requeridas en materia de investigación criminal contra los delitos que afectan la información y los datos.

L.C.R.A. - Liga Colombiana de Radio Aficionados. (http://www.lcra.org.co/)
Colaborar con las autoridades en caso de calamidad pública, perturbación del orden público o de emergencia, en la forma que lo determine el Ministerio de Tecnologías de la Información y las Comunicaciones.

Infraestructura de Firma Digital, si fuera el caso.
Brinda servicios de emisión de Certificados digitales para personas naturales y/o funcionarios públicos, asesoramiento sobre tecnologías relacionadas con Documentos Electrónicos, Firma Digital y Capacitación. (Certicamara, GSE, Andes SCD)

***Superintendencia de Industria y Comercio*.**

A la Superintendencia de Industria y Comercio, corresponde la Protección de la Competencia, Propiedad Industrial, Protección al Consumidor, entre otras.

Dirección Nacional de Derecho de Autor.
A la Dirección Nacional de Derecho de Autor, corresponde la administración del Registro Nacional de Derecho de Autor, el cual tiene por finalidad la inscripción de todo tipo de obras en el campo literario y artístico, así como los actos y contratos relacionados con la enajenación o cambio de dominio de éstas; todo con el fin de otorgar un título de publicidad y seguridad jurídica a los diversos titulares en este especial campo del derecho.

En los intercambios de información de seguridad de la información, no se divulgará información confidencial perteneciente a la UPME a personas no autorizadas.

El intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias, solo se permite cuando se haya firmado un Compromiso de Confidencialidad previo o con aquellas Organizaciones especializadas en temas relativos a la seguridad de la Información cuyo personal está obligado a mantener la confidencialidad de los temas que trata.

Acciones de Despliegue e Implantación:

- Identificar entidades que representen autoridad en temas de seguridad de la información.
- Definir las nuevas normas y requerimientos que las autoridades establecen en el tema de seguridad de la información.
- Evaluar la forma de articular los requerimientos existentes de las entidades y/o autoridades al Sistema de Gestión de la Seguridad de la Información de la Unidad de Planeación Minero Energética (UPME).
- Adoptar los requerimientos existentes previa aprobación del comité designado para tal fin.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PA005

Título de la Política: Gestión de grupos de interés especial - *Ref.: ISO/IEC 27001 CL A.6.1.4*

Definición de la Política:
Se deben mantener los contactos apropiados con grupos de interés especiales, otros foros especializados y asociaciones de profesionales en seguridad de la información.

Acciones de Despliegue e Implantación:

- Identificar los grupos de interés especiales de profesionales en seguridad de la información.
- Establecer protocolos de comunicación y responsables para el contacto con los grupos de interés.

Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

7.1.3. Seguridad de los recursos humanos- Ref.: ISO/IEC 27001 CL. A.7

Es de vital importancia concienciar a los funcionarios de la Unidad de Planeación Minero Energética (UPME) sobre la necesidad de generar las condiciones propicias para garantizar la confidencialidad, integridad y disponibilidad de la información, por tal razón se tienen en cuenta los siguientes requisitos para establecer controles efectivos para su realización.

PA006 **Título de la Política: Proceso de Selección – *Ref.: ISO/IEC 27001:2013 CL. A.7.1.1***
Definición de la Política: El área de Gestión del Talento Humano de la Unidad de Planeación Minero Energética (UPME) debe hacerse responsable del cumplimiento de las funciones designadas, con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de la información desde el proceso de preselección hasta el retiro de los funcionarios.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información**.**

PA007 **Título de la Política: Términos y condiciones del empleo - Ref.: ISO/IEC 27001 CL. A. 7.1.2**
Definición de la Política: Los acuerdos contractuales con funcionarios y contratistas deben establecer sus responsabilidades y las de la entidad en cuanto a seguridad de la información.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PA008

Título de la Política: Responsabilidades de la dirección - Ref.: ISO/IEC 27001 CL. A. 7.2.1
Definición de la Política: La dirección debe requerir a todos los funcionarios y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PA009 **Título de la Política: Toma de conciencia, educación y formación en la seguridad de la información - *Ref.: ISO/IEC 27001 CL. A.7.2.2.***
Definición de la Política: La Unidad de Planeación Minero Energética (UPME) debe estar comprometida en adoptar una cultura de seguridad de la información, estableciendo y manteniendo un programa anual de concienciación y capacitación para todos los funcionarios de la entidad, así como para los contratistas y terceros que tengan acceso a la información institucional y desarrollen actividades de manera permanente en sus instalaciones. Esto con el fin de proteger la información y la infraestructura tecnológica que la soporta. Todos los funcionarios, contratistas y demás terceros al servicio de las entidades y dependencias que conforman la entidad, deben ser informados y/o capacitados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas, por medio de procesos de sensibilización y/o guías específicas del SGSI. El personal que ingrese a la UPME recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas de información que correspondan. Por otra parte, se habilitarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.
Acciones de Despliegue e Implantación: ● Definir el programa anual de concienciación y capacitación para todos los funcionarios de la entidad, así como para los contratistas y terceros. ● Ejecutar el programa de acuerdo al programa anual definido.
Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PA010

Título de la Política: Proceso disciplinario Ref.: ISO/IEC 27001:2013 CL. A.7.2.3

Definición de la Política: Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas estatutarias y convencionales que rigen al personal de la Administración Pública Nacional, y en caso de corresponder, se realizarán las acciones correspondientes ante las entidades pertinentes.

Las sanciones solo pueden imponerse mediante un acto administrativo que así lo disponga cumpliendo las formalidades impuestas por los preceptos constitucionales, la Ley de Procedimiento Administrativo y demás normativas específicas aplicables.

Acciones de Despliegue e Implantación:

- Identificar la violación incurrida a las políticas de seguridad de la información.
- Toda violación a las políticas de licenciamiento de software, será motivo de sanciones aplicables al personal que incurra en ésta.
- Cualquier violación a la seguridad por parte del personal que labora en la entidad, así como terceros que tengan relación o algún tipo de contrato con la Unidad de Planeación Minero Energética (UPME), se harán acreedores de sanciones aplicables acorde a la normatividad vigente.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PA011

Título de la Política: Terminación de contrato o cambio de responsabilidad en el empleo – *Ref.: ISO/IEC 27001 CL A.7.3.1.*

Definición de la Política: En el momento de la desvinculación o de cambio de roles o responsabilidades de algún funcionario, contratista y/o tercero de la entidad, se debe hacer entrega de todos los activos de información que le hayan sido asignados mediante el formato establecido.

El área de Gestión del Talento Humano debe notificar a la Oficina de Gestión de la Información de la entidad sobre la desvinculación, cambio de rol o responsabilidad de los colaboradores, para que ésta retire o cambie los derechos (privilegios) de acceso a la información de esos funcionarios.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

7.1.4. Gestión de los activos de información- Ref.: ISO/IEC 27001 CL A.8.

Dentro de las responsabilidades de la Unidad de Planeación Minero Energética (UPME) se encuentra la custodia sobre todo tipo de información generada por la entidad misma o sus dependientes y que genere un impacto dentro de la entidad; así mismo, se monitorea el almacenamiento de documentos o archivos.

PA012 **Título de la Política: Devolución de activos - *Ref.: ISO/IEC 27001 CL A.8.1.4***
Definición de la Política: Todos los servidores y usuarios de partes externas deben devolver todos los activos de la entidad que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PA013 **Título de la Política: Disposición de los medios de soporte- Ref.: ISO/IEC 27001 CL. A. 8.3.2**
Definición de la Política: Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

7.1.5. Relaciones con los proveedores - Ref.: ISO/IEC 27001 CL. A.15

Los proveedores garantizan la confidencialidad e integridad de la información a la cual tengan acceso durante la permanencia en las instalaciones de la entidad.

PA014
Título de la Política: Seguridad de la información para las relaciones con proveedores - Ref.: ISO/IEC 27001 CL. A.15.1.1

Definición de la Política: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la entidad se deben acordar con éstos y se deben documentar, para asegurar la protección de los activos de la Unidad de Planeación Minero Energética (UPME) que sean accesibles a los proveedores:

- Cumplimiento de la Política de seguridad de la información de la UPME.
- Protección de los activos de información de la UPME, incluyendo:

  - Procedimientos para proteger los bienes de la UPME, abarcando los activos físicos, la información y el software.
  - Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
  - Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
  - Restricciones a la copia y divulgación de información.
  - Descripción de los servicios disponibles.
  - Nivel de servicio esperado y niveles de servicio aceptables.
  - Permiso para la transferencia de personal cuando sea necesario.
  - Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
  - Existencia de Derechos de Propiedad Intelectual.
  - Definiciones relacionadas con la protección de datos.
  - Acuerdos de control de accesos que contemplen:

    - Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
    - Proceso de autorización de accesos y privilegios de usuarios.
    - Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

  - Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
  - Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
  - Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.

- Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
- Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.
- Proceso claro y detallado de administración de cambios.
- Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
- Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
- Controles que garanticen la protección contra software malicioso.
- Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.
- Relación entre proveedores y subcontratistas.

- Los proveedores o contratistas que tengan relaciones comerciales con la entidad, se les incluirá dentro de su contrato una cláusula de confidencialidad de información y un acuerdo de confidencialidad de información.
- Los proveedores tendrán acceso limitado a información sensible de la entidad. Si para fines de su labor fuera necesario tener acceso a dicha información, está se proporcionará con ciertas medidas de seguridad, con el fin de que no pueda ser modificada o alterada por el proveedor.
- Los contratistas no podrán tener acceso a áreas o zonas donde se encuentre información sensible en la entidad. Si fuera necesario su ingreso a determinadas áreas, será necesaria la autorización de un funcionario, el cual debe acompañar al contratista durante el tiempo que este permanezca en dicha área.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PA015
Título de la Política: Tratamiento de la seguridad dentro de los acuerdos con proveedores - Ref.: ISO/IEC 27001 CL. A.15.1.2

Definición de la Política: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura para la entidad, teniendo en cuenta los requisitos establecidos en los acuerdos de confidencialidad pactados con el proveedor.

Acciones de Despliegue e Implantación:

- Establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor para el manejo de la información de la Unidad de Planeación Minero Energética (UPME).
- Formalizar estos requisitos en los acuerdos de confidencialidad con cada proveedor.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PA016
Título de la Política: Cadena de suministro de tecnología de información y comunicación.- Ref.: ISO/IEC 27001 CL. A.15.1.3

Definición de la Política: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación para la UPME.

Acciones de Despliegue e Implantación:

- Establecer y acordar todos los requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
- Formalizar estos requisitos en los acuerdos con cada proveedor.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PA017
Título de la Política: Seguimiento y revisión de los servicios de los proveedores. Ref.: ISO/IEC 27001 CL. A.15.2.1

Definición de la Política: La entidad debe realizar revisiones y auditorías periódicas sobre responsabilidades convenidas en el contrato entre el contratista y la Unidad de Planeación Minero Energética (UPME), teniendo en cuenta las obligaciones contractuales establecidas.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PA018 **Título de la Política: Gestión de cambios en los servicios de los proveedores - Ref.: ISO/IEC 27001 CL. A.15.2.2**
Definición de la Política: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información , sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos; así mismo, que la Oficina de Gestión de la Información de la UPME, es quien autoriza los cambios o modificaciones de los servicios prestados por sus proveedores.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes para la gestión de en los servicios prestados por los proveedores.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

7.1.6. Cumplimiento - Ref.: ISO/IEC 27001 CL. A.18

PA019 **Título de la Política: Identificación de la legislación aplicable y de los requisitos contractuales - Ref.: ISO/IEC 27001 CL. A.18.1.1**
Definición de la Política: La entidad debe atender a todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como los requerimientos para cumplirlos. De igual manera se deben identificar y documentar explícitamente los requisitos de la legislación aplicable, y mantenerlos actualizados para el Sistema de Gestión de Seguridad de la Información de la UPME. ● La entidad debe atender a la siguiente normativa: - **Norma ISO/IEC 27001:2013:** Establece las directrices del Sistema de Gestión de la seguridad de la información. Adicionalmente establece el rol y responsabilidad de los funcionarios y grupos de interés de la entidad y establece la metodología de identificación de los activos de información, la valoración de los riesgos, la calificación de los controles, el plan de tratamiento para la mitigación de los riesgos asociados a los activos de información, las revisiones y auditorías que se le hacen al SGSI. ● Los requisitos legales y regulatorios que afectan la seguridad de la información deben ser reconocidos por: - La Alta Dirección. - Los dueños de cada proceso de la entidad. - El Oficial de seguridad de la información.

- Los representantes de otras áreas relacionadas con la seguridad.

Adicionalmente, de manera continua se deben realizar:

- Revisiones permanentes sobre la expedición de nuevas leyes y normatividades que afectan de manera directa la Seguridad de la Información de la entidad.
- La interpretación de las implicaciones en la seguridad de la información de estas leyes y reglamentos.
- La identificación de la posibilidad de incumplimiento legal y reglamentario por parte de la entidad.
- La determinación de acciones sobre el posible incumplimiento.

Acciones de Despliegue e Implantación:

- Identificar y documentar los requisitos de la legislación aplicable.
- Ajustar los requisitos de acuerdo con las actualizaciones normativas que surjan y apliquen para el Sistema de Gestión de Seguridad de la Información en la Unidad de Planeación Minero Energética (UPME).

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PA020
Título de la Política: Derechos de la propiedad intelectual - Ref.: ISO/IEC 27001 CL. A.18.1.2

Definición de la Política: La Unidad de Planeación Minero Energética (UPME) debe implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el registro de derechos de uso.

En la entidad, la política de licenciamiento de software y derechos de propiedad intelectual debe establecer que:

- La entidad debe cumplir con la reglamentación de propiedad intelectual para lo cual implementa los controles necesarios que garanticen el respeto de dicha reglamentación.
- No se permite el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.

- Se permite el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de los mismos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.
- Definición de normas y procedimientos para el cumplimiento de la normatividad vigente.
- Divulgación de las políticas de adquisición de software y las disposiciones de la normatividad vigente.
- Se debe mantener un adecuado registro de activos.
- Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
- Implementar controles para evitar el exceso del número máximo permitido de usuarios.
- Verificar que solo se instalen productos con licencia y software autorizado.
- Elaboración y divulgación de un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
- Utilización de herramientas de auditoría adecuadas.
- Cumplimiento con los términos y condiciones establecidos para obtener software e información en redes públicas.
- La Unidad de Planeación Minero Energética (UPME) debe realizar un inventario de licencias de software mínimo dos veces al año, en particular de herramientas de oficina y productividad, licencia de usuario de sistemas operativos de red, base de datos y otros.
- Se debe tener control sobre el uso de software libre que hacen los usuarios, y su relación con la función que realizan.
- La Unidad de Planeación Minero Energética (UPME) debe hacer seguimiento y control sobre el uso de licencias asignadas a los usuarios, mediante una auditoria según el perfil de usuario de software establecido.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías definidas; para dar cumplimiento a los requisitos legislativos, de reglamentación y contractuales que estén relacionados con los derechos de propiedad intelectual y el registro de derechos de uso.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PA021 **Título de la Política: Protección de registros - Ref.: ISO/IEC 27001 CL. A.18.1.3**
Definición de la Política: Los registros críticos de la UPME se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de la UPME. Los registros se clasificarán en diferentes tipos, por ejemplo, registros contables, registros de base de datos, registros de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo, papel, microfichas, medios magnéticos u ópticos.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes para la protección de registros críticos en la Unidad de Planeación Minero Energética (UPME).
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PA022 **Título de la Política: Privacidad y protección de información de datos personales - Ref.: ISO/IEC 27001 CL. A.18.1.4**
Definición de la Política: Todos los funcionarios deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones. La UPME redactará un “Acuerdo de Confidencialidad”, el cual deberá ser suscrito por los funcionarios. La copia firmada del acuerdo será retenida en forma segura por la UPME. Mediante este instrumento el funcionario se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate. A través del “Acuerdo de Confidencialidad” se deberá advertir al funcionario que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del funcionario (Ver 6. Seguridad del Personal). En particular, se deberán tener presente las siguientes normas: ● Código Penal, Titulo III. Delitos Contra la Administración Pública. **Artículo 148A. - Utilización indebida de información privilegiada. Adicionado.** Ley 190 de 1995, Art. 27.El servidor público o el particular que como funcionario o directivo o miembro de una junta u órgano de administración de cualquier entidad pública o privada que haga uso indebido de información que haya conocido por razón o con ocasión de sus

funciones, con el fin de obtener provecho para sí o para un tercero, sea éste persona natural o jurídica, incurrirá en prisión de dos (2) a seis (6) años e interdicción de funciones por el mismo término de la pena principal. **Art. 154. - Revelación de secreto**. El funcionario oficial que indebidamente dé a conocer documento o noticia que deba mantener en secreto o reserva, incurrirá en arresto de seis (6) meses a cinco (5) años, en multa de un mil a diez mil pesos e interdicción de derechos y funciones públicas de seis (6) meses a dos (2) años. Si del hecho resultare perjuicio, la pena será de uno (1) a cinco (5) años de prisión, multa de cinco mil a veinte mil pesos e interdicción de derechos y funciones públicas hasta por el mismo término. **Art. 155. - Utilización de asunto sometido a secreto o reserva.** El funcionario oficial que utilice en provecho propio o ajeno, descubrimiento científico, u otra información o dato llegados a su conocimiento por razón de sus funciones, y que deban permanecer en secreto o reserva, incurrirá en prisión de seis (6) meses a cuatro (4) años, multa de un mil a diez mil pesos e interdicción de derechos y funciones públicas hasta por el mismo tiempo, siempre que el hecho no constituya otro delito.

- **Artículo 258**. Modificado por la Ley 1474 de 2011, artículo 18. **Utilización indebida de información privilegiada**. El que como funcionario, asesor, directivo o miembro de una junta u órgano de administración de cualquier entidad privada, con el fin de obtener provecho para sí o para un tercero, haga uso indebido de información que haya conocido por razón o con ocasión de su cargo o función y que no sea objeto de conocimiento público, incurrirá en pena de prisión de uno (1) a tres (3) años y multa de cinco (5) a cincuenta (50) salarios mínimos legales mensuales vigentes. En la misma pena incurrirá el que utilice información conocida por razón de su profesión u oficio, para obtener para sí o para un tercero, provecho mediante la negociación de determinada acción, valor o instrumento registrado en el Registro Nacional de Valores, siempre que dicha información no sea de conocimiento público **Artículo 420**. Modificado por la Ley 1288 de 2009, artículo 25.**Utilización indebida de información oficial privilegiada**. El servidor público que, como funcionario o directivo o miembro de una junta u órgano de administración de cualquier entidad pública, que haga uso indebido de información que haya conocido por razón o con ocasión de sus funciones y que no sea objeto de conocimiento público, con el fin de obtener provecho para sí o para un tercero, sea este persona natural o jurídica, incurrirá en pena de prisión de cinco (5) a ocho (8) años y pérdida del empleo o cargo público. **Artículo 431**. **Utilización indebida de información obtenida en el ejercicio de función pública**. El que habiéndose desempeñado como servidor público **durante el año inmediatamente anterior** utilice, en provecho propio o de un tercero, información obtenida en calidad de tal y que no sea objeto de conocimiento público, incurrirá en multa.

- **LEY 909:2004:** Esta Ley redefinió el Sistema General de Información Administrativa del Sector Público, creado mediante la Ley 489 de 1998, y amplió su cobertura a todos los organismos y entidades del poder público, organismos de control, organización electoral y organismos autónomos en los órdenes nacional, departamental, distrital y municipal. Previó la estructura del subsistema de recursos humanos. Este contiene la información sobre el número de empleos públicos, trabajadores oficiales y contratistas de prestación de servicios, novedades de ingreso y retiro y la información sobre los regímenes de bienestar social y capacitación. Reglamentada por los Decreto 3246 de 2007 y 1409 de 2008.

- **LEY 734:2002:** Por la cual se expide el Código Disciplinario Único. Régimen Disciplinario para los Servidores Públicos. Parte III. Derechos y Deberes-Deberes, Derechos, Prohibiciones, Incompatibilidades y Conflicto de Intereses del Servidor Público.

- **LEY 1266:2008:** Protección de Datos Personales. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- **LEY 1273:2009** - Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- **LEY 1581:2012** - La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

- **DECRETO 1377:2013** - El presente Decreto tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

Asimismo, deberá considerarse lo establecido en la Ley 962 de 2005: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Adicionalmente el Decreto 1151/2008: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PTI023

Título de la Política: Reglamentación de controles criptográficos - Ref.: ISO/IEC 27001 CL. A. 18.1.5

Definición de la Política: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PA024 **Título de la Política: Revisión independiente de la seguridad de la información - Ref.: ISO/IEC 27001 CL. A.18.2.1**
Definición de la Política: La Auditoría Interna, Control Interno o en su defecto quien sea designado por el Comité institucional de gestión y desempeño debe realizar revisiones independientes sobre la vigencia e implementación de las Políticas de Seguridad de la Información, a efectos de garantizar que las prácticas de la Unidad de Planeación Minero Energética (UPME) reflejen adecuadamente sus disposiciones, teniendo en cuenta los siguientes parámetros: ● Garantizar la pertinencia de las políticas y lineamientos establecidos para la entidad. ● Evaluar la eficacia, eficiencia y efectividad del SGSI. ● Determinar si existen nuevos requerimientos o actualizaciones de la norma. ● Establecer los cambios y modificaciones que sean necesarias al SGSI. ● Someter a discusión en el comité designado en la entidad los cambios a realizar. ● Aprobar y dejar documentado las modificaciones realizadas al SGSI.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PA025 **Título de la Política: Revisión y cumplimiento de las políticas y normas de seguridad - *Ref.: ISO/IEC 27001 CL. A.18.2.2 y A.18.2.3***
Definición de la Política: El oficial de seguridad debe velar por el cumplimiento del procesamiento y procedimientos de gestión de la información dentro de la Unidad de Planeación Minero Energética (UPME), con las políticas y normas de seguridad

apropiadas. Así mismo los funcionarios deben dar cumplimiento a las políticas y normas de seguridad.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes para posibilitar que el Oficial de Seguridad vele por una adecuada gestión de la información. En caso de ser identificado algún tipo de incumplimiento de las políticas o normas de seguridad, el Oficial de Seguridad debe realizar lo siguiente: ● Establecer las causas del incumplimiento. ● Evaluar las acciones correctivas adecuadas para tratar las causas que generan el incumplimiento. ● Determinar la acción correctiva escogida. ● Revisar y hacer seguimiento al plan de tratamiento o acción de mejora emprendida.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

7.2. Políticas concernientes a la Oficina de Gestión de la Información de la Unidad de Planeación Minero Energética (UPME). (PTI)

Las siguientes Políticas de Seguridad de la Información son responsabilidad de la Oficina de Gestión de la Información de la entidad según la NTC ISO/IEC 27001:2013.

7.2.1. Políticas de seguridad de la información - Ref.: ISO/IEC 27001 CL. A.5.

PETI001 **Título de la Política: Políticas para la administración del riesgo en la seguridad de la información- - *Ref.: ISO/IEC 27001 CL. A.5.1.***
Definición de la Política: El dueño de proceso de la Oficina de Gestión de la Información de la Unidad de Planeación Minero Energética (UPME) debe identificar, analizar y evaluar los riesgos asociados a sus activos de información, al mismo tiempo implementar acciones tanto correctivas como preventivas establecidas en el plan de tratamiento del SGSI. De igual manera, los funcionarios de la entidad tienen conocimiento de los riesgos de cada activo de información, con el fin de gestionar el riesgo de manera oportuna, garantizando así los principios de confidencialidad, integridad y disponibilidad de la información.
Acciones de Despliegue e Implantación:

● Identificar los activos de información por parte de la Oficina de Gestión de la Información de la Unidad de Planeación Minero Energética (UPME). ● Implementar una metodología de gestión del riesgo (transversal a la entidad y para seguridad de la información) con el fin de identificar los planes de tratamiento adecuados a aplicar de manera oportuna.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI002 **Título de la Política: Seguridad de la información en la gestión de proyectos- Ref.: ISO/IEC 27001 CL. A. 6.1.5**
Definición de la Política: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI003 **Título de la Política: Política para los dispositivos móviles - *Ref.: ISO/IEC 27001 CL A.6.2.1***
Definición de la Política: Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, la Oficina de Gestión de la Información de la entidad debe implementar controles de acceso, técnicas criptográficas para cifrar la información crítica almacenada en estos, mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la seguridad de la información.
Acciones de Despliegue e Implantación: ● Definir los mecanismos de autorización y conexión de dispositivos móviles que no son propiedad de la Unidad de Planeación Minero Energética (UPME) y quien necesite hacer uso de sus redes.

• Definir las acciones determinantes para la protección de los datos, determinando que datos se guardan y dónde. Si los sistemas empresariales necesitan guardar datos en el equipo móvil, deben dictaminarse políticas pertinentes para su cifrado y posterior eliminación cuando ya no sean demandados.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI004 **Título de la Política: Teletrabajo - Ref.: ISO/IEC 27001 CL. A. 6.2.2**
Definición de la Política: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
Acciones de Despliegue e Implantación: • Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

7.2.2. Gestión de los activos de información- Ref.: ISO/IEC 27001 CL A.8.

Dentro de las responsabilidades de la Unidad de Planeación Minero Energética (UPME) se encuentra la custodia sobre todo tipo de información generada por la entidad misma o sus dependientes y que genere un impacto dentro de la UPME, así mismo se monitorea el almacenamiento de documentos o archivos.

PETI005 **Título de la Política: Inventario de activos - *Ref.: ISO/IEC 27001 CL A.8.1.1***
Definición de la Política: La Unidad de Planeación Minero Energética (UPME) debe identificar los activos asociados con la información e instalaciones de procesamiento de información, y debe elaborar y mantener un inventario de estos activos. Todos los activos de información: Software, hardware, servicios, bases de datos o cualquier otro que sea diseñado o desarrollado para la entidad, de manera directa o indirecta con ocasión de convenios o contratos con organismos públicos, gubernamentales o entidades particulares o privadas, son de propiedad de la Unidad de Planeación Minero Energética (UPME) y hacen parte del inventario de activos de la entidad.

Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI006 **Título de la Política: Propiedad de los activos - *Ref.: ISO/IEC 27001 CL A.8.1.2***
Definición de la Política: Los activos de información deben tener un propietario o responsable asociado, quien velará por su buen uso y custodia.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI007 **Título de la Política: Uso aceptable de los activos - *Ref.: ISO/IEC 27001 CL A.8.1.3***
Definición de la Política: Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información, así como las instalaciones de procesamiento de la misma. Los funcionarios de la entidad deben hacer buen uso de los activos de información designados para su labor dentro de la entidad.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI008 **Título de la Política: Clasificación de la información - *Ref.: ISO/IEC 27001 CL. A.8.2.1***
Definición de la Política: La información debe ser clasificada por la Unidad de Planeación Minero Energética (UPME), en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

Toda la información debe ser identificada, clasificada y documentada por los propietarios de los activos de información, siendo ellos los responsables de establecer y clasificar los mismos, dentro de las siguientes categorías:

- **PUBLICO:** Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea funcionario de la UPME o no.

- **RESERVADA – USO INTERNO:** Información que puede ser conocida y utilizada por todos los funcionarios de la UPME y algunas personas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la UPME, el Sector Minero Energético o terceros.

- **RESERVADA – CONFIDENCIAL:** Información que solo puede ser conocida y utilizada por un grupo de funcionarios, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la UPME, el Sector Minero Energético o a terceros.

- **RESERVADA SECRETA:** Información que solo puede ser conocida y utilizada por un grupo muy reducido de funcionarios, generalmente directivos de la UPME, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves a la UPME, el Sector Minero Energético o a terceros.

Acciones de Despliegue e Implantación:

- La Unidad de Planeación Minero Energética (UPME) debe identificar, clasificar y documentar la información sobre los activos de información que son asignados a cada uno de sus funcionarios.
- Dar cumplimiento al procedimiento de identificación y clasificación de activos de información.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI009

Título de la Política: Etiquetado de la información - Ref.: ISO/IEC 27001 CL. A. 8.2.2

Definición de la Política: Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
- Para realizar el etiquetado de los Activos de Información se proponen los siguientes lineamientos:

  - Se deben etiquetar todos los Activos de Información que estén clasificados según

el esquema clasificación en Confidencialidad, Integridad y disponibilidad de la Entidad.

- Si un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado en todos sus niveles (Confidencialidad, Integridad y Disponibilidad) como NO CLASIFICADA.
- Para los activos clasificados en confidencialidad como INFORMACION PUBLICA RESERVADA se podría utilizar la etiqueta IPR, INFORMACION PUBLICA CLASIFICADA IPC y INFORMACION PUBLICA, IPB.
- Para los activos clasificados en integridad como ALTA se utilizará la etiqueta A, MEDIA, M y BAJA, B.
- Para los activos clasificados en disponibilidad como ALTA se utilizará la etiqueta 1, MEDIA, 2 y BAJA, 3.

De esta manera se realizarían las combinaciones de acuerdo con los criterios de clasificación de la información.

Fecha de Creación: Mayo de 2021

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI010

Título de la Política: Manejo de activos- Ref.: ISO/IEC 27001 CL. A. 8.2.3

Definición de la Política: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Mayo de 2021

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI011

Título de la Política: Gestión de medios removibles - *Ref.: ISO/IEC 27001 CL. A.8.3.1*

Definición de la Política: Se debe restringir la conexión no autorizada de cualquier elemento de almacenamiento externo, como dispositivos personales USB, discos duros externos, CDs, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, módems, entre otros dispositivos no institucionales o no autorizados por la entidad.

Los medios de almacenamiento removibles como cintas, discos duros removibles, CDs, DVDs, medios impresos y dispositivos USB, entre otros, que contengan información institucional, deben ser controlados y físicamente protegidos.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI012 **Título de la Política: Transferencia de medios de soporte físicos- Ref.: ISO/IEC 27001 CL. A. 8.3.3**
Definición de la Política: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

7.2.3. Control de accesos- Ref.: ISO/IEC 27001 CL. A.9

Para la Unidad de Planeación Minero Energética (UPME) debe ser prioritario definir el personal que tenga acceso a información sensible, por lo cual ha limitado el acceso de usuarios de aplicaciones computarizadas únicamente a los funcionarios y demás personal tanto interno como externo que tengan que ver directamente con sus responsabilidades y funciones u obligaciones a cargo, debido a que la información puede ser sensible o tener un carácter confidencial. Así mismo, es necesario restringir el acceso a las instalaciones donde dicha información se encuentra guardada, garantizando así la confidencialidad, disponibilidad e integridad de la misma.

PETI014 **Título de la Política: Política de control y Administración de accesos - *Ref.: ISO/IEC 27001 CL. A.9.1.1***

Definición de la Política: La Unidad de Planeación Minero Energética (UPME) debe establecer que los funcionarios, contratistas, pasantes y demás personal que tenga acceso a la información de la entidad:

- Son usuarios de la red de la entidad todos los funcionarios, trabajadores oficiales, los trabajadores en misión, los contratistas, los pasantes y terceros, bien sea personas naturales o empresas que estén de forma temporal o permanente en la Unidad de Planeación Minero Energética (UPME).
- El acceso a la red por parte de terceros debe estar estrictamente restringido y permisible únicamente con previa autorización del encargado de brindar acceso a la red de la entidad.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política de accesos a la información, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI015

Título de la Política: Seguridad para Internet.- - *Ref.: ISO/IEC 27001 CL. A.9.1.2*

Definición de la Política: El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

El responsable de la Seguridad de la Información definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el responsable del Área Funcional a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

Se evaluará la conveniencia de generar un registro de los accesos de los usuarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares. Dicho control será comunicado a los usuarios de acuerdo con lo establecido en el punto “Acuerdo de Confidencialidad”. Para ello, el Responsable de la Seguridad de la Información junto con el Responsable de la Oficina de Gestión de la Información analizarán las medidas a ser implementadas para efectivizar dicho control, como la instalación de “Firewalls”, “WAF”, “Proxies”, etc.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política y reglas sobre el uso de internet en la Unidad de Planeación Minero Energética (UPME), mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI015

Título de la Política: Seguridad para redes inalámbricas. - - *Ref.: ISO/IEC 27001 CL. A.9.1.2*

Definición de la Política: Para tener acceso a cualquier red inalámbrica, los funcionarios, contratistas y demás personas que se conecten a las redes inalámbricas de la entidad deben:

- Conectarse a las redes inalámbricas en la red de la entidad a través de protocolos seguros.
- Conectarse a las redes inalámbricas que estén habilitadas en zonas desmilitarizadas, destinadas para este propósito.
- Acceder a la red inalámbrica de la entidad los usuarios y equipos autorizados mediante la asociación de las direcciones MAC de los portátiles a las direcciones IP asignadas.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política de accesos y seguridad en las redes inalámbricas de la Unidad de Planeación Minero Energética (UPME), mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI016

Título de la Política: Administración de cuentas - *Ref.: ISO/IEC 27001 CL. A.9.2.1*

Definición de la Política: En la Unidad de Planeación Minero Energética (UPME), los funcionarios, contratistas, pasantes, funcionarios en misión o cualquier persona deben pasar por un proceso formal de registro y/o de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política de gestión de cuentas en los sistemas de información, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
- Firmar un Acuerdo de Confidencialidad por parte de los funcionarios, contratistas, pasantes, funcionarios en misión o cualquier persona deben pasar por un proceso formal de registro, en el cual se determine el tiempo de vigencia de la cuenta, así como el perfil del usuario que va a usar.
- Identificar que el nivel de acceso otorgado a los servicios de red e informáticos de la UPME, es el adecuado para el cumplimiento del propósito de la función asignada al usuario.
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la UPME o sufrieron la pérdida/robo de sus credenciales de acceso.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI017 **Título de la Política: Suministro de acceso de usuarios - Ref.: ISO/IEC 27001 CL. A. 9.2.2**
Definición de la Política: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI018 **Título de la Política: Gestión de derechos de acceso privilegiado - Ref.: ISO/IEC 27001 CL. A. 9.2.3**
Definición de la Política: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI019 **Título de la Política: Gestión de información de autenticación secreta de usuarios- Ref.: ISO/IEC 27001 CL. A. 9.2.4**
Definición de la Política: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI020 **Título de la Política: Revisión de los derechos de acceso de usuario- Ref.: ISO/IEC 27001 CL. A. 9.2.5**
Definición de la Política: Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares. Se deben validar los derechos de acceso a los activos periódicamente.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI021 **Título de la Política: Cancelación o ajuste de los derechos de acceso- Ref.: ISO/IEC 27001 CL. A. 9.2.6**
Definición de la Política: Los derechos de acceso de todos los servidores y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI022 **Título de la Política: Uso de información de autenticación secreta- Ref.: ISO/IEC 27001 CL. A. 9.3.1**
Definición de la Política: Se debe exigir a los usuarios que cumplan las prácticas de la entidad para el uso de información de autenticación secreta.
Acciones de Despliegue e Implantación:

● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI023 **Título de la Política: Restricción de acceso a información- Ref.: ISO/IEC 27001 CL. A. 9.4.1**
Definición de la Política: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política de control de acceso, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI024 **Título de la Política: Procedimiento de conexión segura- Ref.: ISO/IEC 27001 CL. A. 9.4.2**
Definición de la Política: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política de control de acceso, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI025 **Título de la Política: Política de Gestión de contraseñas- *Ref.: ISO/IEC 27001 CL.* A.9.4.3**
Definición de la Política: El responsable de la Seguridad de la Información definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

- Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo funcionario. El uso de identificadores grupales solo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
- Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
- Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad de la UPME, por ejemplo, que no compromete la separación de tareas.
- Entregar a los usuarios un detalle escrito de sus derechos de acceso.
- Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
- Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
- Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la UPME o sufrieron la pérdida/robo de sus credenciales de acceso.
- Efectuar revisiones periódicas con el objeto de:
  - ✓ Cancelar identificadores y cuentas de usuario redundantes.
  - ✓ Inhabilitar cuentas inactivas por más de 30 días.
  - ✓ Eliminar cuentas inactivas por más de 60 días.
- En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.
- Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
- Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones, si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política de contraseñas (basado en buenas prácticas), mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI026

Título de la Política: Uso de programas utilitarios privilegiados- Ref.: ISO/IEC 27001 CL. A. 9.4.4

Definición de la Política: Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

Acciones de Despliegue e Implantación:

● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI027 **Título de la Política: Control de acceso a códigos fuente de programas- Ref.: ISO/IEC 27001 CL. A. 9.4.5**
Definición de la Política: Se debe restringir el acceso a códigos fuente de programas.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

7.2.4. Criptografía - Ref.: ISO/IEC 27001 CL. A. 10

Con el fin de garantizar la confidencialidad e integridad de algunos documentos designados como sensibles, la entidad utilizará sistemas y técnicas criptográficas para la protección de la información.

PETI028 **Título de la Política: Política sobre el uso de controles criptográficos (Protección de la Información) - Ref.: ISO/IEC 27001 CL. A. 10.1.1**
Definición de la Política: El sistema de información debe implementar mecanismos de protección de información que cumplan con la reglamentación, políticas, estándares, guías aplicables, así: Mediante la evaluación de riesgos que llevará a cabo el Propietario de la Información y el responsable de la Seguridad de la Información, se identificará el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar. Al implementar la Política del Organismo en materia criptográfica, se considerarán los controles aplicables a la exportación e importación de tecnología criptográfica. ● Proporcionar una protección adecuada a los equipos utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

● Proteger las claves secretas y privadas evitando que sean copiadas o modificadas sin autorización.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política relacionada con el cifrado de datos, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI029 **Título de la Política Gestión de llaves - Ref.: ISO/IEC 27001 CL. A. 10.1.2**
Definición de la Política: Se debe implementar en la Unidad de Planeación Minero Energética (UPME) un sistema de administración de claves criptográficas para garantizar la confidencialidad, disponibilidad e integridad de la información sensible de la entidad; para lo cual, las claves criptográficas se convierten en un activo de información esencial, garantizando así que tanto el emisor como el receptor de la información, envían y reciben información fidedigna, veraz e integra.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política del manejo de llaves de cifrado, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

7.2.5. Seguridad de las operaciones - Ref.: ISO/IEC 27001 CL. A. 12

Se protege la seguridad de las operaciones en las instalaciones de procesamiento de la información, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

PETI030 **Título de la Política: Operaciones documentadas - Ref.: ISO/IEC 27001 CL. A. 12.1.1**
Definición de la Política: Se debe documentar y mantener actualizados todos los procedimientos de operación, teniendo en cuenta los ya existentes en la entidad, asegurando la disponibilidad de la información. Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el responsable de la Seguridad de la Información.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

- Procesamiento y manejo de la información.
- Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
- Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
- Restricciones en el uso de utilitarios del sistema.
- Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
- Instrucciones especiales para el manejo de “salidas”, como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.
- Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

Acciones de Despliegue e Implantación:

- Definir y documentar los procedimientos de operación.
- Divulgar los procedimientos de operación a los funcionarios de la Unidad de Planeación Minero Energética (UPME).
- Actualizar los procedimientos de operación con una frecuencia definida o cuando se requiera un ajuste significativo.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI031

Título de la Política: Gestión de cambios - Ref.: ISO/IEC 27001 CL. A. 12.1.2

Definición de la Política: Se debe mantener un control de los cambios en la entidad, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información y se debe justificar la razón de dichos cambios, los cuales serán revisados y evaluados por parte de la Oficina de Gestión de la Información de la entidad, el Oficial de Seguridad y las partes interesadas en la entidad.

El responsable de la Seguridad de la Información procurará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El Jefe de la Oficina de Gestión de la Información evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

Se retendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios contemplarán los siguientes puntos:

- Identificación y registro de cambios significativos.
- Evaluación del posible impacto de dichos cambios.
- Aprobación formal de los cambios propuestos.
- Planificación del proceso de cambio.
- Prueba del nuevo escenario.
- Comunicación de detalles de cambios a todas las personas pertinentes.
- Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI032

Título de la Política: Gestión de capacidad - Ref.: ISO/IEC 27001 CL. A. 12.1.3

Definición de la Política: La Oficina de Gestión de la Información de la entidad o la persona que sea designada por el área realizará una revisión periódica sobre las necesidades de capacidad de las instalaciones y de los sistemas de procesamiento de la información, debiéndose proyectar las necesidades futuras de capacidad adicional, a fin de garantizar un procesamiento y almacenamiento adecuado y suficiente.

Por lo anterior, se deben evaluar las necesidades actuales de almacenamiento de información y hacer una proyección de los requerimientos de capacidad en el futuro con el fin de que se generen acciones preventivas, donde se pueda gestionar el riesgo asociado a la falta o disminución capacidad de almacenamiento de información, comprometiendo la disponibilidad de la misma. Además, se deben tener en cuenta las siguientes medidas:

- Implementación de los mecanismos, controles y herramientas necesarias para asegurar que los recursos que componen dicha plataforma sean periódicamente monitoreados, afinados y proyectados para futuros requerimientos de capacidad de procesamiento y comunicación.
- El responsable de cada componente de la plataforma tecnológica debe realizar el monitoreo permanente sobre éste.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI033

Título de la Política: Separación de los ambientes de desarrollo, de pruebas y operación. - Ref.: ISO/IEC 27001 CL. A. 12.1.4

Definición de la Política: Se deben establecer roles y responsabilidades en cada fase del desarrollo o modificación de los sistemas de información de la entidad y a su vez se deben separar los ambientes de desarrollo, pruebas y producción, con el fin de garantizar la integridad y disponibilidad de la información.

Se deben proveer los mecanismos, controles y recursos necesarios para contar con niveles adecuados de separación lógica y/o física entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica y sistemas de información, con el fin de reducir el acceso no autorizado y evitar cambios que pudieran afectar su operación. Por lo anterior se deben tomar en consideración los siguientes factores:

- El paso de software de un ambiente a otro se controla y gestiona.
- Los usuarios cuentan únicamente con los privilegios necesarios en cada ambiente para el desarrollo de sus funciones.
- No se realizan pruebas, instalaciones o desarrollos de software directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad o confidencialidad de la información.
- El ambiente del sistema de prueba emula el ambiente de producción lo más estrechamente posible.
- No se permite la copia de información reservada, confidencial, restringida o exclusiva de la entidad, desde el ambiente de producción al ambiente de pruebas; en caso de que sea estrictamente necesario, la copia la autoriza el propietario de la información y el Oficial de Seguridad de la Información y se implementan controles que garanticen que la confidencialidad de la información sea protegida y se elimine de forma segura después de su uso.
- Se restringe el acceso a los compiladores, editores, utilidades de los sistemas y otras herramientas de desarrollo desde los sistemas del ambiente de producción y a cualquier usuario que no lo requiera para el desarrollo de su labor.
- Periódicamente se verifican las versiones instaladas tanto en ambiente de pruebas como en producción y confrontan esta información con revisiones previas y con las versiones de programas fuentes almacenadas en los repositorios de la cada dependencia.
- Se establecen roles y responsabilidades en cada fase del desarrollo o modificación de los sistemas de información de la entidad y a su vez se separan los ambientes de desarrollo, pruebas y producción, con el fin de garantizar la integridad y disponibilidad de la información.

Acciones de Despliegue e Implantación: Aplicar, divulgar y monitorear el cumplimiento de la política para el ciclo de desarrollo y cambio a programas, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI034 **Título de la Política: Controles contra códigos maliciosos- Ref.: ISO/IEC 27001 CL. A. 12.2.1**
Definición de la Política: Para asegurarse de que la información y las instalaciones de procesamiento de la información estén protegidos contra códigos maliciosos se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia de protección de los usuarios contra códigos maliciosos. Estos controles deberán considerar las siguientes acciones: ● Prohibir el uso de software no autorizado para la UPME. ● Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar. ● Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria. ● Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas). ● Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la UPME, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas. ● Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables. ● Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos. ● Concientizar al personal acerca del problema de los falsos virus y de cómo proceder frente a los mismos.
Acciones de Despliegue e Implantación: Aplicar, divulgar y monitorear el cumplimiento de la política de antivirus, antimalware, antispam y en general códigos maliciosos, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI035

Título de la Política: Respaldo de la información. - Ref.: ISO/IEC 27001 CL. A. 12.3.1

Definición de la Política: El Jefe de la Oficina de Gestión de la Información o a quien este delegue dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Para esto, se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico de la UPME. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades de la UPME.

Se definirán procedimientos para el resguardo de la información, que deberán considerar los siguientes puntos:

- Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
- Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo con lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.
- Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para la UPME. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad.
- Asignar a la información de resguardo un nivel de protección física y ambiental según las especificaciones aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
- Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos; como mínimo una vez por año.

Acciones de Despliegue e Implantación:

Aplicar, divulgar y monitorear el cumplimiento de la política de copias de respaldo y recuperación de información, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI036
Título de la Política: Registro de eventos - Ref.: ISO/IEC 27001 CL. A. 12.4.1

Definición de la Política: Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.

Los registros de auditoría deberán incluir:

- Identificación del usuario.
- Fecha y hora de inicio y terminación.
- Id UPME o ubicación de la terminal, si se hubiera dispuesto identificación automática para la misma.
- Registros de intentos exitosos y fallidos de acceso al sistema.
- Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos de la Política de Retención de Registros.

Los Propietarios de la Información junto con la Oficina de Control Interno o en su defecto quien sea propuesto por el Comité institucional de gestión y desempeño, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

Acciones de Despliegue e Implantación:

Aplicar, divulgar y monitorear el cumplimiento de esta política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI037
Título de la Política: Protección de la información de registro - Ref.: ISO/IEC 27001 CL. A. 12.4.2

Definición de la Política: La Oficina de Gestión de la Información de la entidad en conjunto con el Oficial de Seguridad de la Información, los propietarios de los riesgos asociados a los activos de información deben establecer los criterios necesarios que permiten el aseguramiento de la información, basados en el nivel de criticidad de cada activo de la entidad. Por tal razón, las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.

Acciones de Despliegue e Implantación:

Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI038 **Título de la Política: Registros del administrador y del operador - Ref.: ISO/IEC 27001 CL. A. 12.4.3**
Definición de la Política: Para garantizar la integridad de la información debe existir un registro de cualquier modificación realizada al sistema de procesamiento de la información; por tal razón, se debe tener en cuenta lo siguiente: ● Llevar un registro documentado en el que se consignen las solicitudes de modificación o de cambios que se hayan realizado a los sistemas de procesamiento de información. ● Documentar de manera clara y explícita cuando hayan ocurrido fallas, la forma como fueron corregidas y el porcentaje de avance de la acción de mejora
Acciones de Despliegue e Implantación: Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI039 **Título de la Política: Sincronización de relojes- Ref.: ISO/IEC 27001 CL. A. 12.4.4**
Definición de la Política: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI040

Título de la Política: Gestión de las vulnerabilidades técnicas - Ref.: ISO/IEC 27001 CL. A. 12.6.1
Definición de la Política: Con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de la información en el sistema de información y procesamiento de la información se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen, evaluar la exposición de la entidad a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
Acciones de Despliegue e Implantación: Aplicar, divulgar y monitorear el cumplimiento de la política de gestión de las posibles vulnerabilidades técnicas, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI041 **Título de la Política: Restricciones sobre la instalación y/o actualización de software - Ref.: ISO/IEC 27001 CL. A. 12.6.2 y A. 12.5.1**
Definición de la Política: Los funcionarios de la Unidad de Planeación Minero Energética (UPME), no podrán instalar ningún software, programa o aplicativo en los equipos designados para su labor en la entidad o bajo la modalidad de teletrabajo. En el caso en que se requiera su instalación, el servidor debe pedir la autorización a su jefe inmediato, justificando de forma escrita la necesidad de la instalación del nuevo software. Cuando sea autorizado por el jefe inmediato, El le escalará el requerimiento a la Oficina de Gestión de la Información de la entidad siendo la única área autorizada para la instalación del nuevo software en los equipos de la entidad.
Acciones de Despliegue e Implantación: Aplicar, divulgar y monitorear el cumplimiento de la política y reglas sobre instalación y actualización de software en la Unidad de Planeación Minero Energética (UPME), mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI042 **Título de la Política: Controles sobre auditorías de sistemas de información- Ref.: ISO/IEC 27001 CL. A. 12.7.1**
Definición de la Política: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.

Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

7.2.6. Seguridad de las comunicaciones - Ref.: ISO/IEC 27001 CL. A. 13

Es de vital importancia la transmisión de información desde y hacia la entidad, por tal razón se establecen ciertos parámetros que garantizan la confidencialidad e integridad de la información.

PETI043 **Título de la Política: Control de redes - Ref.: ISO/IEC 27001 CL. A. 13.1.1**
Definición de la Política: El acceso a las redes de la Unidad de Planeación Minero Energética (UPME) debe estar limitado a los funcionarios de la entidad y demás personas autorizadas por la misma por medio de claves de acceso a los sistemas de información, con la finalidad de disminuir el acceso no autorizado de personal ajeno a la entidad.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política de gestión de redes, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI044 **Título de la Política: Seguridad de los servicios de red - Ref.: ISO/IEC 27001 CL. A. 13.1.2**
Definición de la Política: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, ya sea que los servicios se presten internamente o se contraten externamente. Con el fin de garantizar la confidencialidad e integridad de la información se deben establecer las siguientes medidas: ● Mantener instalados y habilitados solo aquellos programas, aplicativos o servicios que sean utilizados por los funcionarios de la entidad o demás personas autorizadas para su manejo. ● Controlar el acceso lógico a los programas, aplicativos o servicios tanto de los usuarios como de los administradores.

- Configurar cada programa, aplicativo o servicio de manera segura, evitando las vulnerabilidades que se pudieran presentar.
- Instalar y verificar periódicamente las actualizaciones de seguridad realizadas.

Acciones de Despliegue e Implantación:

Aplicar, divulgar y monitorear el cumplimiento de las políticas relacionadas con los servicios de red, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI045

Título de la Política: Separación de redes - Ref.: ISO/IEC 27001 CL. A. 13.1.3

Definición de la Política: La arquitectura de red de la Unidad de Planeación Minero Energética (UPME) debe considerar la separación de redes de acuerdo con el nivel de confidencialidad y la clase de información que se almacena en los sistemas que constituyen dichas redes.

Acciones de Despliegue e Implantación:

Aplicar, divulgar y monitorear el cumplimiento de la política relacionado con la segmentación de las redes, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI046

Título de la Política: Transferencia de la información - Ref.: ISO/IEC 27001 CL. A.13.2.1

Definición de la Política: Se debe prohibir el envío de información confidencial o sensible de la entidad a personal externo de la Unidad de Planeación Minero Energética (UPME) sin autorización previa.

- Está prohibido el uso del correo electrónico personal (Hotmail, Gmail...) para el envío o recepción de cualquier tipo de información relacionada con la entidad.
- Cualquier información que entre o salga de la Unidad de Planeación Minero Energética (UPME) por medio magnético, transmisión electrónica o hardware, deberá tener los mecanismos de autenticación, autorización y registro de los eventos que aseguren la confidencialidad, integridad, auditabilidad y disponibilidad de esta información.

Acciones de Despliegue e Implantación:

Aplicar, divulgar y monitorear el cumplimiento de la política para transferir información, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI047

Título de la Política: Acuerdos sobre transferencia de información - Ref.: ISO/IEC 27001 CL. A. 13.2.2

Definición de la Política: Se debe contar con procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones, en concordancia con la normatividad vigente.

Las alianzas y convenios con los proveedores estarán regidos bajo los siguientes criterios:

- Cualquier alianza o convenio de procesamiento de información con proveedores o con personal externo a la entidad debe contar con mecanismos de confidencialidad, integridad y auditabilidad de tal forma que cumpla con los estándares definidos por seguridad de la información de la entidad.
- La información referente a servicios, trámites e información entre la Unidad de Planeación Minero Energética (UPME) y los usuarios de la página Web, debe tener la seguridad necesaria para el uso de registro de usuarios, gestión de sesiones seguras, generación de registros de auditoría y validez jurídica para dar pleno valor probatorio a los mensajes de datos.
- Para todo el intercambio de información confidencial o restringida se deben establecer acuerdos de confidencialidad.

Acciones de Despliegue e Implantación:

Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI048

Título de la Política: Mensajería electrónica - Ref.: ISO/IEC 27001 CL. A.13.2.3

Definición de la Política: Con el fin de garantizar la confidencialidad de la información, se deben establecer parámetros para el envío de la información a terceros por medio del correo electrónico de la entidad para proteger adecuadamente la información incluida en la mensajería electrónica, para tal fin:

- Los funcionarios de la Unidad de Planeación Minero Energética (UPME) serán responsables de todas las actividades realizadas con su cuenta de correo institucional.
- Los funcionarios de la Unidad de Planeación Minero Energética (UPME) no entregarán, ni compartirán la clave del correo institucional asignado para el desarrollo de sus funciones a otros funcionarios ni a terceras personas.
- En el caso de recibir un correo electrónico de un destinatario desconocido, este no debe ser abierto y el empleado debe notificar de forma inmediata, para evitar que en caso de que este contenga algún virus, infecte el sistema.
- El servicio de correo electrónico debe ser usado únicamente para el ejercicio de las funciones de competencia de cada usuario.
- El uso indebido del servicio de correo electrónico es motivo de suspensión temporal de su cuenta de correo o la eliminación total de la cuenta dentro del sistema.
- La Unidad de Planeación Minero Energética (UPME) se reserva el derecho de monitoreo del servicio de correo electrónico el cual será realizado por el Oficial de Seguridad de la Información en conjunto con la Alta Dirección.

Acciones de Despliegue e Implantación:

Aplicar, divulgar y monitorear el cumplimiento de la política del uso de la mensajería electrónica (SMS, Whatsapp, BBM, entre otros), mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI049

Título de la Política: Acuerdos de confidencialidad o de no divulgación - Ref.: ISO/IEC 27001 CL. A.13.2.4

Definición de la Política: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la entidad para la protección de la información.

En todo convenio o contrato que la Unidad de Planeación Minero Energética (UPME) firme con sus funcionarios, contratistas, pasantes y demás personal será necesario:

- Establecer un Acuerdo de Confidencialidad de la Información.
- En el caso de los funcionarios, al momento de la posesión del cargo, deberán firmar un Acuerdo de confidencialidad y reserva de la información a la cual tengan acceso mientras este vigente su vínculo laboral con la UPME.
- En el caso de los contratistas, se les incluirá dentro de los contratos, un Acuerdo de confidencialidad y reserva de la información a la cual tengan acceso mientras permanezcan en la UPME.

Acciones de Despliegue e Implantación:

Aplicar y monitorear el cumplimiento del acuerdo de confidencialidad para funcionarios, contratistas, pasantes y demás personal.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

7.2.7. Adquisición, desarrollo y mantenimiento de sistemas - Ref.: ISO/IEC 27001 CL. A. 14

Con la finalidad de garantizar la continuidad del negocio y la disponibilidad de la información se establecen las siguientes directrices:

PETI050 **Título de la Política: Adquisición y Mantenimiento de Sistemas- Ref.: ISO/IEC 27001 CL. A.14.1**
Definición de la Política: La Unidad de Planeación Minero Energética (UPME) debe asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.
Acciones de Despliegue e Implantación: Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI051 **Título de la Política: Análisis y especificación de requisitos de seguridad de la información- Ref.: ISO/IEC 27001 CL. A.14.1.1**
Definición de la Política: La Unidad de Planeación Minero Energética (UPME) 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.
Acciones de Despliegue e Implantación: Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI052 **Título de la Política: Seguridad de servicios de las aplicaciones en redes públicas. - Ref.: ISO/IEC 27001 CL. A.14.1.2**
Definición de la Política: La Oficina de Gestión de la Información de la entidad debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas, la información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas.
Acciones de Despliegue e Implantación: Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI053 **Título de la Política: Protección de transacciones de los servicios de las aplicaciones. - Ref.: ISO/IEC 27001 CL. A.14.1.3**
Definición de la Política: 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 autorizada por medio de controles que establecerá la Oficina de Gestión de la Información de la entidad.
Acciones de Despliegue e Implantación: Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI054 **Título de la Política: Política de desarrollo seguro- Ref.: ISO/IEC 27001 CL. A. 14.2.1**
Definición de la Política: Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas dentro de la entidad.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021

Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI055 **Título de la Política: Procedimientos de control de cambios en sistemas- Ref.: ISO/IEC 27001 CL. A. 14.2.2**
Definición de la Política: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI056 **Título de la Política: Revisión técnica de las aplicaciones después de cambios en la plataforma de operación - Ref.: ISO/IEC 27001 CL. A.14.2.3**
Definición de la Política: Cuando se cambian las plataformas de operación, la Oficina de Gestión de la Información de la entidad debe revisar las aplicaciones críticas del negocio, y someterlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la entidad provocado por los cambios previamente aprobados y ejecutados por la Oficina de Gestión de la Información de la entidad.
Acciones de Despliegue e Implantación: Aplicar, divulgar y monitorear el cumplimiento de la política de cambios de plataforma, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI057 **Título de la Política: Restricciones en los cambios a los paquetes de software - Ref.: ISO/IEC 27001 CL. A.14.2.4**
Definición de la Política: Los cambios a los paquetes de software son autorizados, supervisados y realizados por funcionarios de la Oficina de Gestión de la Información 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.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política de cambios de la plataforma de la operación, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI058

Título de la Política: Principios de organización de sistemas seguros- Ref.: ISO/IEC 27001 CL. A. 14.2.5

Definición de la Política: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Mayo de 2021

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI059

Título de la Política: Ambiente de desarrollo seguro- Ref.: ISO/IEC 27001 CL. A. 14.2.6

Definición de la Política: Las entidades deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Mayo de 2021

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI060

Título de la Política: Desarrollo contratado externamente- Ref.: ISO/IEC 27001 CL. A. 14.2.7
Definición de la Política: La entidad debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI061

Título de la Política: Pruebas de seguridad de sistemas - Ref.: ISO/IEC 27001 CL. A.14.2.8

Definición de la Política: 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 de la Oficina de Gestión de la Información de la entidad.

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

- **Pruebas de compatibilidad**: Se debe garantizar el funcionamiento adecuado y continúo del software desarrollado en diferentes plataformas: hardware, sistemas operativos, redes.

- **Pruebas de integración**: Se debe 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.

- **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.

- **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.

- **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.

- **Pruebas integrales de seguridad**: Estas pruebas enumeran las mejores prácticas que se deben evaluar a nivel de cada aplicación:

Recopilación de Información; Pruebas de gestión de la configuración; Pruebas de la lógica de negocio; Pruebas de Autenticación; Pruebas de Autorización; Pruebas de gestión de sesiones; Pruebas de validación de datos; Pruebas de denegación de Servicio; Pruebas de Servicios Web; Pruebas de AJAX.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política para la realización de las pruebas de seguridad de la información, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI062 **Título de la Política: Prueba de aceptación de sistemas- Ref.: ISO/IEC 27001 CL. A. 14.2.9**
Definición de la Política: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba y criterios relacionados.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI063 **Título de la Política: Protección de datos de prueba- Ref.: ISO/IEC 27001 CL. A. 14.3.1**
Definición de la Política: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

7.2.8. Gestión de incidentes de seguridad de la información - Ref.: ISO/IEC 27001 CL. A.16

La Unidad de Planeación Minero Energética (UPME) gestiona los incidentes de forma eficaz y eficiente, de tal forma que se disminuya el impacto que se pudiera generar en la entidad.

PETI064 **Título de la Política: Responsabilidades y procedimientos - Ref.: ISO/IEC 27001 CL. A.16.1.1**
Definición de la Política: La Unidad de Planeación Minero Energética (UPME) debe establecer acciones que mitiguen el impacto asociado a los incidentes que se presentan; por tal razón, se establecerán los procedimientos para la gestión de los incidentes de seguridad de la información.
Acciones de Despliegue e Implantación: Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI065 **Título de la Política: Reporte de eventos de seguridad de la información - Ref.: ISO/IEC 27001 CL. A.16.1.2**
Definición de la Política: Los usuarios de servicios de información, al momento de tener conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al responsable de la Seguridad de la Información. Se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política relacionada con la gestión de eventos, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI066

Título de la Política: Informe de debilidades de seguridad de la información - Ref.: ISO/IEC 27001 CL. A. 16.1.3
Definición de la Política: Se debe requerir a todos los funcionarios y contratistas que usan los servicios y sistemas de información de la entidad, que informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI067 **Título de la Política: Evaluación de eventos de seguridad de la información y decisiones sobre ellos - Ref.: ISO/IEC 27001 CL. A.16.1.4**
Definición de la Política: La Unidad de Planeación Minero Energética (UPME) debe probar periódicamente (por lo menos una vez al año), la capacidad de respuesta a incidentes del sistema de información para determinar la efectividad de la respuesta al incidente y documenta los resultados.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política para las pruebas relacionadas con seguridad de la información, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI068 **Título de la Política: Respuesta a incidentes de seguridad de la información- Ref.: ISO/IEC 27001 CL. A. 16.1.5**
Definición de la Política: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI069 **Título de la Política: Aprendizaje obtenido de los incidentes de seguridad de la información - Ref.: ISO/IEC 27001 CL. A.16.1.6**
Definición de la Política: Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PETI070 **Título de la Política: Recolección de evidencia. - Ref.: ISO/IEC 27001 CL. A.16.1.7**
Definición de la Política: La Unidad de Planeación Minero Energética (UPME) debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
Acciones de Despliegue e Implantación: Aplicar, divulgar y monitorear el cumplimiento de la política para obtención de evidencias, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

7.2.9. Aspectos de seguridad de la información de la gestión de continuidad del negocio - Ref.: ISO/IEC 27001 CL. A.17

La Unidad de Planeación Minero Energética (UPME) implementa un proceso de continuidad del negocio con la finalidad de mitigar el impacto de acciones como desastres naturales, accidentes, fallas de los equipos y acciones deliberadas de terceros en los cuales la entidad no tiene injerencia directa, pero establece acciones para poder recuperarse rápidamente y que la operación de la entidad no se vea comprometida.

PETI071
Título de la Política: Planificación de la continuidad de la seguridad de la información - Ref.: ISO/IEC 27001 CL. A.17.1.1

Definición de la Política: El Comité institucional de gestión y desempeño, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades de la UPME.

Este Comité tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información de la UPME frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

- Identificar y priorizar los procesos críticos de las actividades de la UPME.
- Asegurar que todos los integrantes de la UPME comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad de la UPME.
- Elaborar y documentar una estrategia de continuidad de las actividades de la UPME consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad de las actividades de la UPME de conformidad con la estrategia de continuidad acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades de la UPME.
- Proponer las modificaciones a los planes de contingencia.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la gestión de continuidad de seguridad de la información, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI072
Título de la Política: Implementación de la continuidad de la seguridad de la información - Ref.: ISO/IEC 27001 CL. A.17.1.2

Definición de la Política: Los propietarios de procesos y recursos de información, con la asistencia del responsable de la Seguridad de la Información, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades de la UPME. Estos procesos deberán ser propuestos por el Comité institucional de gestión y desempeño.

El proceso de planificación de la continuidad de las actividades considerará los siguientes puntos:

- Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.
- Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.
- Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.
- Documentar los procedimientos y procesos acordados.
- Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
- Instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:

  - Objetivo del plan.
  - Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
  - Procedimientos de divulgación.
  - Requisitos de la seguridad.
  - Procesos específicos para el personal involucrado.
  - Responsabilidades individuales.

- Probar y actualizar los planes.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades de la UPME requeridos, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

Acciones de Despliegue e Implantación:

Aplicar, divulgar y monitorear el cumplimiento de la gestión de continuidad de seguridad de la información, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI073
Título de la Política: Verificación, revisión y evaluación de la continuidad de la seguridad de la información - Ref.: ISO/IEC 27001 CL. A.17.1.3

Definición de la Política: Debido a que los planes de continuidad de las actividades de la UPME pueden fallar, por suposiciones incorrectas, errores o cambios en el equipamiento, se establecen las siguientes pautas de acción:

- El Comité institucional de gestión y desempeño establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.
- El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado Comité.

Se deberán utilizar diversas técnicas para garantizar que los planes de contingencia funcionarán ante un hecho real, y éstas incluirán por lo menos:

- Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación las actividades utilizando ejemplos de interrupciones).
- Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).
- Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia).
- Realizar ensayos completos probando que la UPME, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas de la UPME se tomarán en cuenta, además, los siguientes mecanismos:

- Efectuar pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades de la UPME en paralelo, con operaciones de recuperación fuera del sitio principal).
- Realizar pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con los compromisos contraídos).

Los planes de continuidad de las actividades de la UPME serán revisados y actualizados periódicamente, para garantizar su eficacia permanente. Se incluirán procedimientos en el programa de administración de cambios de la UPME para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades.

La periodicidad de revisión de los planes de contingencia es la siguiente: Cada uno de los responsables de Procesos es el responsable de las revisiones periódicas de cada uno de los planes de continuidad de su incumbencia, como así también de la identificación de cambios en las disposiciones relativas a las actividades de la UPME aún no reflejadas en dichos planes.

Deberá prestarse atención, especialmente, a los cambios de:

- Personal.
- Direcciones o números telefónicos.
- Estrategia de la UPME.
- Ubicación, instalaciones y recursos.
- Legislación.
- Contratistas, proveedores y clientes críticos.
- Procesos, o procesos nuevos / eliminados.
- Tecnologías.
- Requisitos operacionales.
- Requisitos de seguridad.
- Hardware, software y otros equipos (tipos, especificaciones, y cantidad).
- Requerimientos de los sitios alternativos.
- Registros de datos vitales.

Todas las modificaciones efectuadas serán propuestas por el Comité institucional de gestión y desempeño para su aprobación por el superior jerárquico que corresponda.

Por otra parte, el resultado de este proceso será dado a conocer a fin de que todo el personal involucrado tenga conocimiento de los cambios incorporados.

Acciones de Despliegue e Implantación:

Aplicar, divulgar y monitorear el cumplimiento de la gestión de continuidad de seguridad de la información, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PETI074

Título de la Política: Disponibilidad de las instalaciones de procesamiento de información - Ref.: ISO/IEC 27001 CL. A.17.2.1

Definición de la Política: Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad dentro de la Oficina de Gestión de la Información de la entidad.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política de las instalaciones de procesamiento, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

7.3. Políticas concernientes a infraestructura (servicios administrativos) de la Unidad de Planeación Minero Energética (UPME). (PI)

Las siguientes Políticas de Seguridad de la Información son responsabilidad del Área Administrativa según la NTC ISO/IEC 27001:2013.

7.3.1. Seguridad física y del entorno- Ref.: ISO/IEC 27001 CL. A. 11

La seguridad física y del entorno disminuye los daños producidos por interferencias en la consulta o envío la información, adicionalmente se protege la información que se custodia o se procesa dentro de la entidad. Asimismo, permite disminuir el acceso no autorizado de personas con la intención de alterar o modificar la información.

PI001 **Título de la Política: Perímetro de seguridad física - Ref.: ISO/IEC 27001 CL. A. 11.1.1**
Definición de la Política: Para evitar el acceso no autorizado a espacios considerados como sensibles dentro de la entidad se deben tener perímetros de seguridad para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. ● Definir y documentar claramente el perímetro de seguridad. ● Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo, no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo, mediante mecanismos de control, vallas, alarmas, cerraduras, etc. ● Verificar la existencia de un área de recepción atendida por personal. El acceso a dichas áreas y al edificio estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa. ● Extender las barreras físicas necesarias desde el piso inferior hasta el piso superior, a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, por incendio, humedad e inundación. • Identificar claramente todas las puertas de emergencia en caso de incendio o desastre natural. El responsable de la Seguridad de la Información llevará un registro actualizado de los sitios protegidos, indicando: ● Identificación del Edificio y Área. ● Principales elementos a proteger.

- Medidas de protección física.

Acciones de Despliegue e Implantación:

Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PI002

Título de la Política: Controles de Accesos Físicos - Ref.: ISO/IEC 27001 CL. A. 11.1.2

Definición de la Política: Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el responsable de la Seguridad de la Información junto con el Jefe de la Oficina de Gestión de la Información, a fin de permitir el acceso solo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

- Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Solo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
- Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán los siguientes controles de autenticación para autorizar y validar todos los accesos: (por ejemplo: personal de guardia con listado de personas habilitadas o por tarjeta magnética o inteligente y número de identificación personal (PIN), etc.). Se mantendrá un registro protegido para permitir auditar todos los accesos.
- Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.
- Revisar y actualizar cada seis (6) meses los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el responsable de la Unidad Funcional de la que dependa.
- Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Oficina de Control Interno o en su defecto quien sea propuesto por el Comité institucional de gestión y desempeño.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política de acceso físico en la Unidad de Planeación Minero Energética (UPME), mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PI003

Título de la Política: Seguridad de las oficinas, recintos e instalaciones - Ref.: ISO/IEC 27001 CL. A. 11.1.3

Definición de la Política: Para la selección y el diseño de un área protegida se deben establecer las zonas de la entidad donde se maneja de forma permanente información sensible o confidencial la cual debe ser protegida para salvaguardar la confidencialidad, integridad y disponibilidad de la información, teniendo en cuenta los siguientes parámetros:

- Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
- Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán una discrecionalidad mínima de su propósito, sin signos obvios, exteriores o interiores.
- Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida para evitar solicitudes de acceso, los cuales podrían comprometer la información.
- Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en la parte exterior o presenten riesgos especiales.
- Implementar los siguientes mecanismos de control para la detección de intrusos: sensores de movimiento, cámaras y dispositivos biométricos. Los mismos serán instalados según estándares profesionales y probados periódicamente. Estos mecanismos de control comprenderán todas las puertas exteriores y ventanas accesibles.
- Separar las instalaciones de procesamiento de información administradas por la UPME de aquellas administradas por terceros.
- Almacenar los materiales peligrosos o combustibles en las bodegas propias o alquiladas a una distancia prudencial de las áreas protegidas de la UPME. Los suministros, como los útiles de escritorio, no serán trasladados al área protegida hasta que sean requeridos.
- Almacenar los equipos redundantes y la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

Acciones de Despliegue e Implantación:

Aplicar, divulgar y monitorear el cumplimiento de la política de acceso físico a áreas sensibles o restringidas de la entidad, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PI004 **Título de la Política: Protección contra amenazas externas y ambientales- Ref.: ISO/IEC 27001 CL. A. 11.1.4**
Definición de la Política: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PI005 **Título de la Política: Trabajo en áreas seguras - Ref.: ISO/IEC 27001 CL. A. 11.1.5**
Definición de la Política: Para garantizar la confidencialidad de la información se hace necesario establecer áreas seguras dentro de la Unidad de Planeación Minero Energética (UPME), por tal razón se deben establecer controles tanto para los funcionarios de la entidad, como para los terceros que tengan acceso a estas zonas de la entidad de acuerdo con los siguientes parámetros: ● Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, solo si es necesario para el desarrollo de sus funciones. ● Evitar la ejecución de trabajos por parte de terceros sin supervisión. ● Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas. ● Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas. ● Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad. ● Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el Responsable de dicho área o el Jefe de la Oficina de Gestión de la Información y el Responsable de la Seguridad de la Información. ● Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.
Acciones de Despliegue e Implantación:

Aplicar, divulgar y monitorear el cumplimiento de la política asociada, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PI006 **Título de la Política: Áreas de despacho y carga- Ref.: ISO/IEC 27001 CL. A. 11.1.6**
Definición de la Política: Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PI007 **Título de la Política: Ubicación y protección de los equipos - Ref.: ISO/IEC 27001 CL. A. 11.2.1**
Definición de la Política: Los equipos deben ser ubicados y protegidos para salvaguardar la integridad y disponibilidad de la información, garantizándole el acceso únicamente al personal autorizado para su uso teniendo en cuenta los siguientes aspectos: ● Ubicar los equipos en zonas de la entidad donde se minimice el acceso de personal no autorizado. ● Ubicar las instalaciones de procesamiento y almacenamiento de información que contienen información confidencial o sensible, en una zona que permita la supervisión durante su uso. ● Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
Acciones de Despliegue e Implantación: Aplicar, divulgar y monitorear el cumplimiento de la política de protección de equipos, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PI008

Título de la Política: Servicios de suministro - Ref.: ISO/IEC 27001 CL. A. 11.2.2

Definición de la Política: Los equipos deben estar protegidos con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía deberá estar de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

- Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
- Contar con un suministro de energía interrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la UPME. La determinación de dichas operaciones críticas será el resultado del análisis de impacto realizado por el responsable de la Seguridad de la Información juntamente con los Propietarios de la Información con incumbencia. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.
- Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Deberá realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa. Dicho análisis será realizado por el responsable de la Seguridad de la Información juntamente con los Propietarios de la Información. Se dispondrá de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

Asimismo, se procurará que los interruptores de emergencia se ubiquen cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se implementará protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

Acciones de Despliegue e Implantación:

Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PI009 **Título de la Política: Seguridad del cableado- Ref.: ISO/IEC 27001 CL. A. 11.2.3**
Definición de la Política: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño, mediante las siguientes acciones: ● Cumplir con los requisitos técnicos vigentes en la República de Colombia (RETIE). ● Utilizar producto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información. ● Proteger el cableado de red contra intercepción no autorizada o daño mediante los siguientes controles: (ejemplo: el uso de conductos o evitando trayectos que atraviesen áreas públicas). ● Separar los cables de energía de los cables de comunicaciones para evitar interferencias.
Acciones de Despliegue e Implantación: Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PI010 **Título de la Política: Mantenimiento de equipos - Ref.: ISO/IEC 27001 CL. A. 11.2.4**
Definición de la Política: Se debe realizar el mantenimiento de los equipos para asegurar la continuidad de la operación y a su vez garantizar la disponibilidad e integridad de la información de forma continua; para lo cual, es necesario realizar el mantenimiento preventivo a los equipos de la entidad, de acuerdo con los intervalos de servicio establecidos y atendiendo a las recomendaciones y especificaciones técnicas establecidas por el fabricante o el proveedor. La Oficina de Gestión de la Información de la entidad mantendrá un control actualizado de la frecuencia de realización del mantenimiento preventivo de los equipos. Adicionalmente se debe tener en cuenta las siguientes los siguientes aspectos: ● Establecer que solo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en los equipos. ● Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado. ● Registrar el retiro de equipamiento de la sede de la UPME para su mantenimiento.

- Eliminar la información confidencial que contenga cualquier equipo que sea necesario retirar, realizándose previamente las respectivas copias de respaldo.

Finalmente debe hacerse una esterilización de los medios de almacenamiento que el equipo tenga, mediante un borrador seguro a traves de una herramienta que permita esta funcionalidad.

Acciones de Despliegue e Implantación:

Aplicar, divulgar y monitorear el cumplimiento de la política de mantenimiento de los equipos, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PI011

Título de la Política: Retiro de activos - Ref.: ISO/IEC 27001 CL. A. 11.2.5

Definición de la Política: Los equipos, información o software no se deben retirar de su sitio sin autorización previa; por lo tanto, debe existir un control.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Mayo de 2021

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PI012

Título de la Política: Seguridad de equipos y activos fuera del predio- Ref.: ISO/IEC 27001 CL. A. 11.2.6

Definición de la Política: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la entidad, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.

Acciones de Despliegue e Implantación:

- Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

Fecha de Creación: Mayo de 2021

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

PI013 **Título de la Política: Disposición segura o reutilización de equipos- Ref.: ISO/IEC 27001 CL. A. 11.2.7**
Definición de la Política: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre escrito. Se debe tener un control establecido sobre los equipos para evitar cualquier pérdida de la información.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PI014 **Título de la Política: Equipos de usuario desatendido- Ref.: ISO/IEC 27001 CL. A. 11.2.8**
Definición de la Política: Los usuarios deben asegurarse que a los equipos desatendidos se les da protección apropiada.
Acciones de Despliegue e Implantación: ● Aplicar, divulgar y monitorear el cumplimiento de la política, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Mayo de 2021
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

PI015 **Título de la Política: Escritorio limpio y pantalla limpia- Ref.: ISO/IEC 27001 CL. A. 11.2.9**
Definición de la Política: Se debe adoptar por parte de la Unidad de Planeación Minero Energética (UPME) una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, con las siguientes acciones: ● Almacenar bajo llave cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo. ● Guardar bajo llave la información sensible o crítica de la UPME (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.

● Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo; tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción. ● Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas. ● Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo. ● Retirar inmediatamente la información sensible o confidencial, una vez impresa. ● Toda vez que un funcionario se ausenta de su lugar de trabajo, junto con bloquear su estación de trabajo, debe guardar en lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial. ● Si el funcionario está ubicado cerca de zonas de atención de público, al ausentarse de su lugar de trabajo deben guardar también los documentos y medios que contengan información de uso interno. ● Las estaciones de trabajo y equipos portátiles deben tener aplicado el estándar relativo a protector de pantalla, de forma que se active el protector definido por la UPME. El primer periodo de cierre corresponderá a los 5 minutos de inactividad en el PC, tras lo cual se activará el protector de pantalla, con mensajes acordes a las buenas prácticas de seguridad.
Acciones de Despliegue e Implantación: Aplicar, divulgar y monitorear el cumplimiento de la política de escritorio y pantalla despejada, mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

8. NORMAS DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y LAS COMUNICACIONES (TIC)

Una norma de la seguridad de la información sustenta una política de seguridad y regula parte o la totalidad del objetivo de la misma.

Actualización de normas

Cualquier solicitud de modificación al documento de Políticas de Seguridad de la Información de la Unidad de Planeación Minero Energética (UPME) debe ser realizada por el Comité institucional de gestión y desempeño.

Estructura de la Norma

La estructura de la Norma es:

- Título de la norma.
- Políticas relacionadas.
- Objetivo.
- Alcance.
- Descripción.
- Fecha de Creación
- Fecha de Actualización
- Aprobado Por:

Reglas de escritura de las normas

- Las normas se escribirán en forma sencilla y en su texto indicarán que es una definición general y aplicable a la Unidad de Planeación Minero Energética (UPME).
- El enunciado debe ser corto, bien redactado y conciso, además debe utilizar términos y palabras que sean de uso común.
- Se mantendrán los términos de seguridad definidos y expresados dentro del documento.

8.1. Normas concernientes a la administración de la Unidad de Planeación Minero Energética (UPME). (NA).

Las siguientes Normas de Seguridad de la Información son responsabilidad de la Administración de la Unidad de Planeación Minero Energética (UPME) según la NTC ISO/IEC 27001:2013.

NA001 **Título de la Norma: Roles y responsabilidades para la seguridad de la información - *Ref.: ISO/IEC 27001 CL A.6.1.1.***
Políticas Relacionadas: Organización de la seguridad de la información y Organización interna.
Objetivo: Definir las responsabilidades que tienen las diferentes áreas dentro del Sistema de Gestión de Seguridad de la Información de la Unidad de Planeación Minero Energética (UPME).
Alcance: Esta norma deberá ser considerada por todos los funcionarios que intervienen dentro del Sistema de Gestión de Seguridad de la Información de la entidad.
Descripción: La Alta Dirección de la Unidad de Planeación Minero Energética (UPME), estará comprometida con el Sistema de Gestión de Seguridad de la Información, por lo cual propenderá por lo siguiente: ● Establecimiento de objetivos dentro del Sistema de Gestión de Seguridad de la Información, que sean coherentes con el objetivo general de la entidad.

- Control por parte de la dirección del Sistema de Gestión de Seguridad de la Información, se realizará a través de revisiones periódicas, las cuales serán planificadas, cumpliendo con los requerimientos del SGSI y de la entidad.

- Establecimiento y aprobación de una política de Seguridad de la Información, la cual debe ser publicada y divulgada a toda la entidad.

- Implementación de acciones tanto preventivas como correctivas que permitan la mitigación de los riesgos potenciales.

- Revisión y modificación de ser necesario el presente documento de Políticas y Normas de Seguridad de la Información de manera periódica.

Comité institucional de gestión y desempeño

Revisar y proponer a la Dirección General de la UPME para su aprobación, la Política y las funciones generales en materia de seguridad de la información.

- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro de la UPME.
- Coordinar el proceso de administración de la continuidad de la operación diaria de los sistemas de tratamiento de la información de la UPME frente a interrupciones imprevistas.

Gestión de tecnología.

Es responsabilidad de la Oficina de Gestión de la Información de la entidad de la Unidad de Planeación Minero Energética (UPME):

- Promover el cumplimiento por parte del personal bajo su responsabilidad de las políticas de seguridad de información.
- Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de seguridad de información.
- Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de seguridad de la información.

- Diseñar, desarrollar, instalar y mantener las aplicaciones bajo su responsabilidad de acuerdo con la metodología establecida e incluyendo los controles de seguridad de información.
- Establecer, documentar y dar mantenimiento a los procedimientos de seguridad que apliquen para la plataforma de tecnologías de información administrada por esta gerencia.
- Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo.
- Establecer y dar mantenimiento a los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.
- Evaluar los procesos o actividades sobre las plataformas tecnológicas, delegados en terceros.
- Implementar y administrar los controles de seguridad sobre los datos y conexiones de la red bajo su administración.
- Definir y gestionar programas de capacitación y entrenamiento que incluyan temas relevantes y pertinentes sobre seguridad de información.
- Custodiar la información y los medios de almacenamiento bajo su responsabilidad.
- Operar y administrar los recursos de cómputo, de red y de software bajo su responsabilidad.

Gestión de riesgos de Seguridad de la Información

- El objetivo de la Gestión de riesgos es identificar y evaluar los riesgos de seguridad de la información a los cuales están expuestos los activos de la entidad, para identificar y aplicar el plan de tratamiento más adecuado.
- La evaluación de riesgos está basada en el impacto y probabilidad de ocurrencia de estos para la entidad y los requerimientos de los niveles de seguridad, tomando en cuenta los controles existentes.
- El análisis y evaluación de riesgos debe hacerse al menos una vez al año.
- El detalle de la metodología de riesgos se encuentra en el capítulo Metodología de Análisis de Riesgos de Seguridad de la Información (Basado en la metodología de NTC-ISO 31000:2009 y ISO/IEC 27005:2011).

Dueños de los procesos

Los dueños de los procesos tienen como funciones las siguientes: Definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados a su proceso, incluyendo aquellas actividades que sean consideradas como controles de seguridad de la información dentro de dichos procedimientos.

Propietarios de los riesgos (Líderes de los Procesos)

Es responsabilidad de los propietarios del riesgo:

- Clasificar sus activos de información de acuerdo con los requerimientos de confidencialidad, integridad y disponibilidad.
- Definir los requerimientos de continuidad y de recuperación en caso de desastre.
- Realizar un análisis anual de riesgos para determinar el grado de exposición a las amenazas vigentes y confirmar los requerimientos de confidencialidad, integridad y disponibilidad relacionados con sus activos de Información.
- Definir los requerimientos de seguridad de riesgos para los activos de información bajo su responsabilidad para que se les proporcione un nivel adecuado de protección en conformidad con los estándares, políticas y procedimientos de seguridad de información.
- Determinar y autorizar todos los privilegios de acceso a sus activos de información.
- Revisar los registros y reportes de auditoría para asegurar el cumplimiento con las restricciones de seguridad para sus activos de información. Por medio de la verificación de los resultados de las revisiones y reportar cualquier situación que involucre un incumplimiento o violación a la seguridad de Información, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.
- Participar en la resolución de los incidentes relacionados con el acceso no autorizado o mala utilización de los activos de información bajo su responsabilidad.

Funcionarios, contratistas y/o terceros.

Es responsabilidad de los funcionarios, contratistas y terceros salvaguardar la información institucional de la entidad, garantizando así la confidencialidad, integridad y disponibilidad teniendo como funciones:

- Cumplir fielmente las políticas de seguridad de la información, contempladas en el presente manual.
- Reportar a la mayor brevedad posible y a través de los canales establecidos, la sospecha u ocurrencia de eventos considerados incidentes de seguridad de información.
- Realizar sugerencias a la Alta Dirección para mejorar los procesos relacionados con los activos de información de la entidad y optimizar así el sistema de seguridad de la información.
- Utilizar los sistemas de información y el acceso a la red únicamente para los propósitos indicados en las políticas de seguridad de la información.
- Incorporar la seguridad de información como parte de las actividades y tareas bajo su responsabilidad.
- Conocer las directrices de protección de los activos de información que utilicen.
- Utilizar únicamente software y demás recursos tecnológicos autorizados.

Acciones de Despliegue e Implantación:

- Definir dentro del manual de funciones de la entidad las responsabilidades de seguridad de la información.
- Determinar dentro del perfil de cargos los roles, perfiles y responsabilidades de la seguridad de la información de cada área de la Unidad de Planeación Minero Energética (UPME).

- Divulgar las responsabilidades dentro del SGSI a funcionarios de la Unidad de Planeación Minero Energética (UPME).

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

NA002
Título de la Norma: Separación de deberes

Políticas Relacionadas: Organización de la seguridad de la información y Organización interna.

Objetivo: Realizar la correcta distribución de roles y responsabilidades, atendiendo a la debida segregación de funciones.

Alcance: Esta norma define la manera se realiza la Separación de deberes en la Unidad de Planeación Minero Energética (UPME).

Descripción: Cada área o dependencia funcional de la UPME, de manera autónoma e independiente de otras áreas tiene el compromiso de:

- Tener un inventario actualizado de los activos de información de su área o dependencia.
- Gestionar los riesgos identificados, asociados a cada activo de información.
- Efectuar y fortalecer los controles establecidos para la gestión efectiva de los riesgos.
- Aprobar y dar curso a las acciones de mejora establecidas con la finalidad de llevar el nivel de riesgo hasta los niveles aceptados por la entidad.

Acciones de Despliegue e Implantación:

- Determinar el inventario de activos de información.
- Identificar los riesgos asociados a los activos de información.
- Establecer los controles necesarios para la gestión de los riesgos.
- Implementar el plan de tratamiento adecuado.
- Monitorear las acciones de mejora definidas.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

NA003
Título de la Norma: Sensibilización

Políticas Relacionadas: Documentación y Entrenamiento.

Objetivo: Programar anualmente un taller de sensibilización en temas de seguridad de Información.

Alcance: Esta norma deberá ser considerada por toda persona que tenga un rol activo en el uso y protección de la información es decir debe ir dirigida a todos los colaboradores de la entidad.
Descripción: Cada colaborador de la Unidad de Planeación Minero Energética (UPME), debe participar de las sesiones de sensibilización sobre seguridad en la información, programadas por la Oficina de Gestión de la Información de la entidad y el Oficial de Seguridad de la Información de la UPME. Para que exista una evidencia de que cada colaborador ha participado en dichas sesiones, debe dejarse un registro de asistencia.
Acciones de Despliegue e Implantación: ● Realizar talleres de sensibilización en seguridad de la información para todos los funcionarios de la entidad. ● Establecer procesos de retroalimentación de las sensibilizaciones realizadas.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

8.2. Normas concernientes a la Oficina de Gestión de la Información de la Unidad de Planeación Minero Energética (UPME).

Las siguientes normas son responsabilidad de la Oficina de Gestión de la Información de la Unidad de Planeación Minero Energética (UPME) según la NTC ISO/IEC 27001:2013.

8.2.1. Administración de Seguridad.

NTI001 **Título de la Norma: Perfiles de Acceso**
Políticas Relacionadas: Acceso a la Información, Administración de la Seguridad de las Tecnologías de Información y las comunicaciones (TIC), Control de Cambios, Privacidad de la Información, Procesamiento de la Información, Responsabilidad del Personal, Uso de Herramientas que Comprometan la Seguridad de las Tecnologías de Información y las comunicaciones (TIC) y Uso de los Recursos de la Infraestructura Tecnológica e Información.
Objetivo: Regular la creación, asignación, cambios y retiros de perfiles de acceso.
Alcance: Esta norma define la manera en que se crea, otorga, cambia y se inactivan los perfiles de acceso que poseen los clientes, a los distintos recursos tecnológicos de la Unidad de Planeación Minero Energética (UPME).

Descripción: Es responsabilidad de la Oficina de Gestión de la Información de la entidad definir, asignar y mantener actualizado los perfiles de acceso a la información en cada una de las aplicaciones de acuerdo con la competencia, el cual es solicitado mediante solicitud escrita por parte del área de Gestión del Talento Humano y/o el jefe del área a la cual vaya a pertenecer el funcionario.

Serán responsables de la administración de los perfiles definidos para la entidad, por tal motivo, debe llevar un registro de los grupos generados, con el significado o función de cada uno de ellos y los clientes y/o recursos que se encuentran asignados a un determinado perfil. Así mismo, debe verificar previo a la ejecución de una solicitud, que no se estén violando políticas o normas de seguridad establecidas y resguardar por un período determinado la información de respaldo.

A partir de la fecha de creación de este documento y con el fin de poder lograr una seguridad homogénea los sistemas de información que se desarrollen o adquieran deben diseñarse de forma tal que permita la administración de perfiles.

Acciones de Despliegue e Implantación:

- Implementar un procedimiento de Gestión de Accesos.
- Restringir la asignación de derechos privilegiados a usuarios autorizados.
- Revisar periódicamente los derechos de acceso asignados y depurar los accesos a los sistemas de información.
- Retirar los privilegios de acceso de los funcionarios que se desvinculan de la entidad.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

NTI002

Título de la Norma: Acceso Controlado a Terceros sobre Recursos Tecnológicos

Políticas Relacionadas: Acceso a la Información, Alianzas o Convenios con Terceros, Conexiones lógicas y eléctricas, Privacidad de la Información, Procesamiento de la Información, Responsabilidad del Personal , Seguridad Física y Uso de los Recursos de la Infraestructura Tecnológica e Información

Objetivo: Regular el acceso de terceros a los recursos tecnológicos de la Unidad de Planeación Minero Energética (UPME).

Alcance: Garantizar un acceso controlado a los recursos tecnológicos de la Unidad de Planeación Minero Energética (UPME).

Descripción: Para dar acceso a un tercero se debe contar con la solicitud a la Oficina de Gestión de la Información de la entidad.

La credencial de visitante es considerada confidencial e intransferible.

El acceso a la red de visitantes de la Unidad de Planeación Minero Energética (UPME) es

validado por la Oficina de Gestión de la Información de la entidad y tendrá un acceso limitado salvo casos especiales.

Acciones de Despliegue e Implantación:

- Establecer protocolos seguros para la conexión a través de redes inalámbricas.
- Capacitar a los usuarios e informar sobre los riesgos asociados al uso de la red inalámbrica.
- Configurar métodos de autenticación adecuados para proteger el acceso inalámbrico al sistema de información.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

NTI003
Título de la Norma: Monitoreo

Políticas Relacionadas: Propiedad de la Información, Responsabilidad del Manejo de Incidentes de Seguridad de las TIC, Responsabilidad de la Seguridad de las TIC, Responsabilidad del Personal y Uso de Herramientas que Comprometan la Seguridad de las TIC.

Objetivo: Realizar las actividades de monitoreo a los diferentes sistemas de la Unidad de Planeación Minero Energética (UPME).

Alcance: Esta norma contempla las actividades de monitoreo que incluye la revisión del log de eventos de los roles que ejecuta cada servidor, donde se almacenan registros, alarmas o errores, para la toma de acciones preventivas o correctivas.

Descripción: El monitoreo se realizará sobre los servidores y los roles que ejecutan.

La Oficina de Gestión de la Información de la UPME debe investigar las nuevas alternativas de monitoreo. En caso de que se considere necesario debe realizar la solicitud de las nuevas herramientas que soporten el monitoreo.

Acciones de Despliegue e Implantación:

- Identificar situaciones que puedan representar un incidente de seguridad.
- Identificar comportamientos anómalos que puedan derivar en un incidente.
- Detectar degradación de los servicios por medio de monitoreo frecuente.
- Verificar el estado de los servidores con una frecuencia definida.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

NTI004
Título de la Norma: Tratamiento de Incidentes de Seguridad

Políticas Relacionadas: Administración de la Seguridad de las TIC, Conexiones Electrónicas, Continuidad, Responsabilidad del Manejo de Incidentes de Seguridad de las TIC, Responsabilidad de la Seguridad de las TIC, Responsabilidad del Personal, Uso de Herramientas que Comprometan la Seguridad de las TIC y Uso de los Recursos de la Infraestructura Tecnológica e Información.
Objetivo: Regular la actuación ante la detección de cualquier incidente de seguridad.
Alcance: Esta norma abarca a todo elemento lógico o físico que se conecte a la Red de la Unidad de Planeación Minero Energética (UPME).
Descripción: La Oficina de Gestión de la Información de la UPME debe coordinar las acciones a seguir para el tratamiento de incidentes de seguridad de las Tecnologías de Información y las comunicaciones (TIC). También debe revisar periódicamente los informes de control de los registros de eventos de los servidores, aplicativos y equipos activos a fin de detectar posibles anomalías y establecer acciones de mejora.
Acciones de Despliegue e Implantación: ● Definir los planes de acción para dar una respuesta oportuna a los incidentes de seguridad. ● Monitoreo las acciones implementadas. ● Llevar un registro documental de las soluciones encontradas para los incidentes que sirva como una base de datos de conocimiento para apoyar el soporte de incidentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

NTI005 **Título de la Norma: Separación de Ambientes y Funciones**
Políticas Relacionadas: Acceso a la Información, Administración de la Seguridad de las TIC, Control de Cambios, Documentación y Entrenamiento, Procesamiento de la Información, Responsabilidad de la Seguridad de las TIC y Responsabilidad del Personal.
Objetivo: Regular la segregación de ambientes y funciones en la infraestructura tecnológica de la Unidad de Planeación Minero Energética (UPME).
Alcance: Esta norma regula la separación de ambientes que deberá existir en la infraestructura tecnológica a fin de proveer una segregación de funciones.
Descripción: Se reconocen los siguientes ambientes básicos: ● **Ambiente de Pruebas:** En este ambiente están involucrados los procesos de la Unidad de Planeación Minero Energética (UPME) a los cuales se deben realizar las pruebas de los sistemas de información con base en una metodología definida para cada caso. Dichas pruebas son necesarias a fin de constatar que los sistemas realizan correcta e integralmente los requerimientos para los que fueron creados. Éste debe ser un ambiente estable, con modificaciones o cambios controlados. Para pasar un sistema, módulo o programa de este ambiente al de producción debe existir una aprobación

formal por parte del Usuario funcional y del funcionario encargado de la Oficina de Gestión de la Información. En este ambiente se deben generar datos de prueba.

- **Ambiente de Producción:** Es el ambiente donde se utilizarán y transformarán los datos de la Unidad de Planeación Minero Energética (UPME). Es el ambiente donde residirá la información operativa de la entidad. No se permite efectuar pruebas sobre este ambiente a excepción de la primera implementación de cada software.

Acciones de Despliegue e Implantación:

- Establecer y proteger el ambiente de preproducción por parte de la Oficina de Gestión de la Información de la entidad.
- Proveer los mecanismos, controles y recursos para la segregación del ambiente de preproducción y producción.
- Establecer los privilegios de acceso a los diferentes ambientes.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

NTI006
Título de la Norma: Software Adquirido

Políticas Relacionadas: Procesamiento de la Información.

Objetivo: Regular la adquisición de cualquier tipo de software para la Unidad de Planeación Minero Energética (UPME).

Alcance: Esta norma contempla todo tipo de software a ser adquirido en la Unidad de Planeación Minero Energética (UPME): Sistema operacional, Bases de datos, software de comunicaciones, utilitarios del sistema, software de seguridad, software de monitoreo, software de oficina y software aplicativo, entre otros.

Descripción: Todo el software de la entidad debe ser legalmente adquirido y se debe contar con las respectivas licencias que lo demuestren.

- Está prohibido para los funcionarios de la Unidad de Planeación Minero Energética (UPME) descargar y/o instalar cualquier tipo de software sin previa autorización.
- Todo software preinstalado en las estaciones de trabajo debe estar licenciado antes de iniciar su uso.
- Para garantizar conformidad con los estándares de seguridad de información propios, se debe adquirir hardware y software a través de canales autorizados.

Acciones de Despliegue e Implantación:

- Realizar capacitaciones sobre las restricciones en la instalación de software a nivel de la entidad.
- Mantener actualizado el inventario de licencias de software de la entidad.

- Determinar los canales autorizados para la adquisición de hardware y software legal.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

NTI007
Título de la Norma: Utilización de claves de Acceso

Políticas Relacionadas: Acceso a la Información, Administración de la Seguridad de las TIC, Conexiones Electrónicas, Cumplimiento de Regulaciones, Documentación y Entrenamiento, Privacidad de la Información, Responsabilidad de la Seguridad de las TIC, Responsabilidad del Personal, Seguridad Física y Uso de los Recursos de la Infraestructura Tecnológica e Información.

Objetivo: Regular el uso y características de las claves de acceso.

Alcance: Esta norma define todos los parámetros genéricos que deben poseer las claves de acceso y el mantenimiento que los clientes internos deben llevar a cabo con las mismas.

Descripción: Todas las credenciales deben tener definida una contraseña, o mecanismo de seguridad que certifique la validez de la misma, a fin de asegurar que el acceso a la infraestructura tecnológica se encuentra debidamente autorizado.

La contraseña es privada, confidencial e intransferible, siendo su titular responsable de evitar su divulgación quien, ante la presunción de que otra persona pudiera conocerla, debe proceder a cambiarla inmediatamente. Se considerará causa grave y será penalizado, el hecho de revelar a otra persona su propia contraseña o solicitar la contraseña de otro usuario.

En la infraestructura tecnológica, las contraseñas deben cumplir con las siguientes características:

- No estén codificadas en programas.
- Deben ser cambiadas periódicamente según la definición del estándar.
- Deben poseer una longitud mínima definida por el estándar (ocho caracteres)
- No se deben repetir por un período de tiempo considerable las mismas contraseñas utilizadas anteriormente
- No deben visualizarse cuando se ingresan.
- Los sistemas de control de acceso deben poseer un diccionario que no permita el ingreso de claves obvias o repetidas.
- Se deben cambiar cada treinta (30) días (caducidad).

Acciones de Despliegue e Implantación:

- Definir y configurar una autenticación por medio de contraseñas robustas.
- Configurar políticas de cambio frecuente de contraseñas.
- Mantener un registro de por lo menos las últimas 10 contraseñas

● Modificar todas las contraseñas por defecto una vez instalado el software y el hardware.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

8.2.2. Seguridad del Software y Hardware

NTI008 **Título de la Norma: Perfiles de Acceso**
Políticas Relacionadas: Acceso a la Información, Administración de la Seguridad de las Tecnologías de Información y las comunicaciones (TIC), Control de Cambios, Privacidad de la Información, Procesamiento de la Información, Responsabilidad del Personal, Uso de Herramientas que Comprometan la Seguridad de las Tecnologías de Información y las comunicaciones (TIC) y Uso de los Recursos de la Infraestructura Tecnológica e Información.
Objetivo: Regular la definición, instalación y mantenimiento de los parámetros de seguridad de la infraestructura tecnológica de la Unidad de Planeación Minero Energética (UPME).
Alcance: Esta norma contempla todos aquellos parámetros relacionados directa o indirectamente con la seguridad de la infraestructura tecnológica de la entidad.
Descripción: La homologación de hardware o software a instalar en la entidad, permite que este sea incorporado respetando los estándares establecidos, logrando de esta forma homogeneidad en los parámetros relativos a la seguridad, permitiendo un control de la infraestructura tecnológica, la facilidad de mantenimiento y monitoreo. La Oficina de Gestión de la Información de la entidad será la responsable de la homologación del hardware y software mediante un proceso de revisión de los parámetros de seguridad vigentes. Es responsabilidad de la Oficina de Gestión de la Información de la entidad mantener actualizado el manual de estándares de seguridad cuando se incorpore una nueva tecnología. Para modificar los estándares establecidos, se debe justificar técnicamente la necesidad, determinar el alcance de la modificación y evaluar el impacto desde el punto de vista de seguridad, con el fin de determinar si debe ser acompañado por otras medidas. Posteriormente y en caso de ejecutarse la modificación, debe registrarse en el formato de control de cambios e implementarse las medidas pertinentes sobre todos los equipos de idénticas características.
Acciones de Despliegue e Implantación: ● Definir el procedimiento para la asignación de perfiles de acceso. ● Establecer el formato de control de cambios.

- Actualizar el manual de estándares de seguridad de la información.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

NTI009

Título de la Norma: Protección de Hardware y Software de Seguridad

Políticas Relacionadas: Administración de la Seguridad de las TIC, Control de Cambios, Continuidad, Privacidad de la Información, Propiedad de la Información, Responsabilidad de la Seguridad de las TIC, Responsabilidad del Personal, Uso de Herramientas que Comprometan la Seguridad de las TIC y Uso de los Recursos de la Infraestructura Tecnológica e Información.

Objetivo: Regular la protección del hardware y software de seguridad.

Alcance: Esta norma abarca a cualquier hardware y software que se utilice exclusivamente para la seguridad de cualquier ambiente, infraestructura, o sistema instalado en la Unidad de Planeación Minero Energética (UPME), ya sea adquirido o de desarrollo propio.

Descripción: Cualquier hardware y software que sea utilizado exclusivamente con fines de seguridad y control, independientemente de su naturaleza, complejidad o modo de adquisición, debe cumplir las siguientes reglas:

- El software de seguridad debe ser utilizado exclusivamente para la Unidad de Planeación Minero Energética (UPME).
- No se podrá desactivar, modificar, instalar versiones diferentes, ni realizar ninguna otra actividad que modifique el comportamiento, en forma alguna, que venía realizando el hardware y software, sin la expresa autorización del Oficial de Seguridad de la entidad.
- La documentación, manuales y cualquier otro tipo de información técnica sobre su comportamiento deben residir en la Oficina de Gestión de la Información de la entidad bajo la responsabilidad de quien designe el jefe de la oficina de Gestión de la Información.
- Ninguna persona podrá transmitir en modo formal o informal, información alguna sobre los parámetros, variables y modo de instalación de ninguna herramienta de seguridad.
- Cualquier incidente sobre estas herramientas de seguridad debe ser informada al Oficial de Seguridad de la entidad, quien debe analizar el incidente, evaluar las posibles consecuencias y tomar las acciones respectivas.

Acciones de Despliegue e Implantación:

- Formalizar y divulgar las reglas para el buen uso de hardware y software.
- Definir los mecanismos para notificar los incidentes sobre las herramientas de seguridad.

Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

NTI010 **Título de la Norma: Uso de Equipos Asignados por la Unidad de Planeación Minero Energética (UPME).**
Políticas Relacionadas: Privacidad de la información, Administración de la Seguridad de las Tecnologías de Información y las comunicaciones (TIC).
Objetivo: Regular el uso de los equipos personales de la Unidad de Planeación Minero Energética (UPME).
Alcance: Esta norma cubre todo equipo de cómputo de uso interno de la entidad que interactúe con la infraestructura tecnológica de la Unidad de Planeación Minero Energética (UPME).
Descripción: Todo software residente en equipo de cómputo o estaciones de trabajo debe estar protegido contra escritura. Todo software debe copiarse antes de iniciar su uso, y esas copias deben almacenarse en un lugar seguro y confiable. Estas copias originales no deben usarse para actividades comerciales ordinarias, sino que deben reservarse para cuando se presenten infecciones de virus, daños en el disco duro y otros problemas en los equipos de cómputo. Los clientes internos de la Unidad de Planeación Minero Energética (UPME) no podrán instalar ningún programa o software desarrollado fuera de la entidad en los equipos o estaciones de trabajo. Los clientes internos de la entidad no podrán almacenar información restringida, confidencial o altamente confidencial en el disco duro del equipo personal o estación de trabajo. La información sensible de la Unidad de Planeación Minero Energética (UPME) tendrá un acceso controlado dependiendo de la fuente de la cual se solicita. Los equipos no deben moverse o reubicarse sin la aprobación previa del Oficial de Seguridad de la entidad. **Nota:** Entiéndase como información sensible: bases de datos, archivos de texto, imágenes o cualquier otro tipo de archivo institucional el cual contenga información expresa de la entidad.
Acciones de Despliegue e Implantación: ● Definir los procedimientos y parámetros para el uso de los equipos designados por la entidad.

- Desarrollar planes de capacitación que informen a los funcionarios sobre el uso adecuado del equipo designado.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

NTI011
Título de la Norma: Copias de Respaldo de Software y Datos de Seguridad

Políticas Relacionadas: Alianzas o Convenios con Terceros, Control de Cambios, Continuidad, Cumplimiento de Regulaciones, Privacidad de la Información, Procesamiento de la Información, Responsabilidad del Personal, Seguridad Física y Uso de los Recursos de la Infraestructura Tecnológica e Información.

Objetivo: Regular la toma de respaldos del software y datos de seguridad.

Alcance: Esta norma abarca a cualquier módulo de control de acceso, herramienta y/o software de seguridad y sus archivos de datos.

Descripción: La Oficina de Gestión de la Información de la Unidad de Planeación Minero Energética (UPME) definirá, para los sistemas y archivos involucrados en la seguridad, los siguientes aspectos:

- La información contenida en los servidores se respalda de forma periódica
- Los medios de las copias de seguridad se almacenan localmente y en un sitio de custodia externa, garantizando en ambos casos la presencia de mecanismos de protección ambiental como detección de humo, fuego, humedad, así como mecanismos de control de acceso físico.
- Las copias de seguridad son probadas periódicamente para garantizar la integridad de la información almacenada y que pueda ser recuperada oportunamente.
- Para garantizar que la información de los funcionarios, contratistas y demás terceros autorizados sea respaldada, es responsabilidad de cada uno mantener copia de la información que se maneje en el recurso compartido definido para cada área y/o usuario
- Los medios de almacenamiento o copias de seguridad del sistema de archivos, o información de la entidad son etiquetados de acuerdo a la información que almacenan haciendo alusión a su contenido.
- Los medios de almacenamiento con información crítica o copias de respaldo son manipulados única y exclusivamente por el personal encargado de hacer los respaldos y su salvaguarda

Acciones de Despliegue e Implantación:

- Definir un esquema de backups apropiado para el respaldo de la información sensible en la Unidad de Planeación Minero Energética (UPME).
- Implementar un sitio de custodia externa para el respaldo de la información.
- Designar el responsable de la manipulación de backups.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

NTI012
Título de la Norma: Cifrado de Datos

Políticas Relacionadas: Alianzas o Convenios con Terceros, Conexiones Electrónicas, Cumplimiento de Regulaciones, Privacidad de la Información, Responsabilidad del Personal y Seguridad Física

Objetivo: Regular la utilización de los métodos de cifrado de información de la Unidad de Planeación Minero Energética (UPME).

Alcance: Esta norma buscará regular la utilización de los métodos de cifrado a ser implementados por la Unidad de Planeación Minero Energética (UPME) en los canales de comunicaciones.

Descripción: Deben utilizarse métodos de cifrado en los casos en que se requiera garantizar que la información operativa de la Unidad de Planeación Minero Energética (UPME) sea transmitida mediante canales de comunicación, de manera que no sea leída o modificada por personas no autorizadas. Se hace necesario implementar el cifrado de documentos para:

- La transmisión de información confidencial o sensible de la entidad hacia entidades o personas externas.
- Cuando haya un acuerdo de confidencialidad con otra entidad o persona sobre la información que se va a transmitir.
- Cuando el propietario del riesgo o el oficial de seguridad de la información consideren un activo de información critico basado en la valoración de riesgo.

Acciones de Despliegue e Implantación:

- Establecer un método de cifrado efectivo para garantizar la confidencialidad de la información.
- Establecer procedimientos para la administración de claves, recuperación de información cifrada pérdida y el restablecimiento de llaves dañadas con el fin de que se garantice la confidencialidad de la clave.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

NTI013
Título de la Norma: Integridad de la Información

Políticas Relacionadas: Procesamiento de la Información, Propiedad de la Información, Responsabilidad del Personal, Uso de Herramientas que Comprometan la Seguridad de las Tecnologías de Información y las comunicaciones (TIC) y Uso de los Recursos de la Infraestructura Tecnológica e Información.

Objetivo: Regular la definición y alcance de los controles que garanticen la integridad de la información.

Alcance: Esta norma contempla todos los equipos de cómputo que procesen información de la Unidad de Planeación Minero Energética (UPME), sean o no de su propiedad y la información transmitida de una fuente a otra con o sin procesamiento.

Descripción: Se deberán tener en cuenta los siguientes controles para los siguientes riesgos:

- **Ingreso de información:** Todo sistema o programa, deberá poseer los controles necesarios que garanticen que la información ingrese en su totalidad de forma precisa, completa y de acuerdo con los tiempos establecidos.
- ***Procesamiento de la información:*** Todo sistema o programa, debe poseer los controles necesarios que garanticen que la información es procesada en su totalidad de forma completa, exacta y en el período estipulado.

Acciones de Despliegue e Implantación:

- Definir controles que garanticen la integridad de la información.
- Detallar y caracterizar tanto el proceso de autenticación como el de validación.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

NTI014

Título de la Norma: Prevención y Detección de Virus

Políticas Relacionadas: Procesamiento de la Información, Responsabilidad del Manejo de Incidentes de Seguridad de las Tecnologías de Información y las comunicaciones (TIC), Responsabilidad del Personal, Uso de Herramientas que Comprometan la Seguridad de las TIC y Uso de los Recursos de la Infraestructura Tecnológica e Información.

Objetivo: Minimizar la pérdida de datos y software a través del ataque de virus informático.

Alcance: Esta norma abarca todo el software de la infraestructura tecnológica y aplicaciones de la Unidad de Planeación Minero Energética (UPME) susceptibles de ser atacados por virus informáticos.

Descripción: En la infraestructura tecnológica que contenga sistemas operativos o aplicaciones, debe implantarse un software antivirus que detecte la presencia de este tipo de ataque. Teniendo en cuenta los siguientes aspectos:

- Prohíbir la instalación o uso de software no autorizado por la UPME.
- Implementar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
- Instalar y actualizar periódicamente el software de detección y reparación de virus, examinando computadores, dispositivos móviles, removibles o cualquier otro dispositivo que contenga información relevante de la entidad.
- Mantener los sistemas de seguridad de la información actualizados.
- Revisar periódicamente el contenido de software de los equipos de procesamiento de la información que sustentan procesos críticos, identificando la presencia de virus o modificaciones no autorizadas en los mismos.

- Verificar la presencia de virus en archivos recibidos de fuentes externas o a través de redes no confiables.
- Concienciar a los funcionarios de la entidad sobre la importancia de verificar el remitente de la información y de los riesgos asociados a los virus que pueden conllevar.

Acciones de Despliegue e Implantación:

- Definir los procedimientos de gestión de sistema de antivirus.
- Monitorear las actualizaciones hechas a los sistemas de información.
- Realizar procesos de capacitación que brinden la información necesaria sobre la prevención y detección de virus.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

NTI015
Título de la Norma: Respaldo de Información

Políticas Relacionadas: Continuidad, Cumplimiento de Regulaciones, Procesamiento de la Información y Seguridad Física.

Objetivo: Regular la toma de respaldo de la información.

Alcance: Esta norma contempla todo tipo de información:

- Datos de las aplicaciones.
- Sistemas de información (programas fuentes y objetos).
- Software de la infraestructura tecnológica.
- Información Técnica.
- Información contenida en los servidores.
- Bases de Datos.

Descripción: Para el software de la infraestructura tecnológica, tanto el proveedor como el profesional de la Unidad de Planeación Minero Energética (UPME) designado para tal fin, deben siempre disponer de una copia de instalación a fin de ser necesario redefinir una infraestructura anterior por necesidades de procesamiento de información histórica.

Toda información crítica o de impacto en la entidad, debe estar respaldada en otros medios magnéticos en un sitio alterno de acuerdo con la norma del Plan de Contingencia y es responsabilidad de la Oficina de Gestión de la Información de la Unidad de Planeación Minero Energética (UPME).

La información debe ser respaldada en una forma organizada mediante el uso de inventarios, catalogación de la información y definición de niveles de respaldo y de forma tal que pueda ser administrada, mantenida y recuperada de sus respaldos cuando la Unidad de Planeación Minero Energética (UPME) necesite hacer uso de ella.

Las copias de respaldo deben siempre estar acompañadas por un procedimiento formalmente definido para ser ejecutado por el Analista de seguridad de la Unidad de Planeación Minero Energética (UPME), designado para tal fin en la periodicidad

definida.
Acciones de Despliegue e Implantación: ● Definir el procedimiento para realización de copias de respaldo. ● Realizar el inventario y gestión de las copias de respaldo existentes. ● Probar de manera periódica las copias existentes para garantizar la integridad de la información mediante la restauración de backups.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

8.2.3. Seguridad de las comunicaciones

NTI016 **Título de la Norma: Accesos Remotos**
Políticas Relacionadas: Acceso a la Información, Alianzas o Convenios con Terceros, Conexiones Electrónicas, Privacidad de la Información, Procesamiento de la Información, Propiedad de la Información y Uso de los Recursos de la Infraestructura Tecnológica e Información.
Objetivo: Especificar el uso de accesos remotos a los recursos informáticos e información de la Unidad de Planeación Minero Energética (UPME).
Alcance: Esta norma contempla todos los accesos remotos que se establezcan con la Red Interna de la Unidad de Planeación Minero Energética (UPME).
Descripción: Todo tipo de acceso remoto que implique comunicación debe realizarse empleando mecanismos de cifrado y autenticación que brinde un escritorio remoto. El trabajo remoto solo será autorizado por el Director General, Secretario General, Subdirectores, Jefes de Oficina de la cual dependa el funcionario que solicite el permiso. Dicha autorización solo se otorgará por la Oficina de Gestión de la Información una vez se verifiquen las condiciones de seguridad del ambiente de trabajo.
Acciones de Despliegue e Implantación: ● Establecer mecanismos de cifrado adecuados. ● Implementar mecanismos de autenticación para acceso remoto.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

NTI017 **Título de la Norma: Seguridad Internet**
Políticas Relacionadas: Acceso a la Información, Administración de la Seguridad de las TIC, Conexiones Electrónicas, Privacidad de la Información, Responsabilidad del Manejo de Incidentes de Seguridad de las TIC, Responsabilidad de la Seguridad de las TIC,

Responsabilidad del Personal, Uso de Herramientas que Comprometan la Seguridad de las TIC y Uso de los Recursos de la Infraestructura Tecnológica e Información.

Objetivo: Definir los aspectos de seguridad a ser aplicadas por la Unidad de Planeación Minero Energética (UPME) en cuanto a la utilización de Internet y las comunicaciones electrónicas a través de esta Red.

Alcance: Esta norma contempla cualquier tipo de comunicación que se establezca a través de Internet por parte de los colaboradores de la Unidad de Planeación Minero Energética (UPME) desde equipos pertenecientes a la Red interna para la realización de tareas operativas.

Descripción: Para el acceso a Internet, los funcionarios, contratistas y demás personas que lo utilicen se comprometen a:

- Acceder a Internet por el canal contratado y aprobado por la entidad. No se autoriza hacer conexiones no controladas ni limitadas hacia Internet.
- Obtener las autorizaciones necesarias para enviar o recibir información confidencial de la Unidad de Planeación Minero Energética (UPME).
- Limitar sin excepción, el acceso a páginas de entretenimiento, pornografía o fuera del contexto laboral.
- Informar en caso de recibir información en archivos adjuntos de dudosa procedencia o que no se esté esperando, al Oficial de Seguridad de la entidad, quién escalará el incidente de seguridad a quién corresponda al interior de la entidad, para analizar y evitar la materialización de cualquier tipo de riesgo que afecte cualquier activo de información.
- Limitar sin excepción la instalación y/o uso de cualquier tipo de juego a través de Internet, así como la utilización de la red para tratar o promover negocios personales.
- Todas las conexiones hacia y desde Internet, deben estar protegidas por el Firewall y en su defecto por la solución WAF; dispuestos para tal fin en la UPME.
- Las conexiones directas de salida a internet no están permitidas.

Adicionalmente, la Unidad de Planeación Minero Energética (UPME) como administrador de la red de Internet, podrá deshabilitar cualquier cuenta de Internet en el momento en que lo considere necesario y más aún cuando la seguridad de la información haya sido violada.

Acciones de Despliegue e Implantación:

- Diseñar guías para el buen uso de internet y las comunicaciones electrónicas a través de la red.
- Restringir el acceso a internet a páginas no requeridas para el desempeño de las funciones en la Unidad de Planeación Minero Energética (UPME).

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

8.2.4. Seguridad física

NTI018 **Título de la Norma: Seguridad Física - Dispositivos de Seguridad Contra Incidencias**
Políticas Relacionadas: Administración de la Seguridad de las TIC, Conexiones Electrónicas, Responsabilidad del Manejo de Incidentes de Seguridad de las TIC, Responsabilidad de la Seguridad de las TIC, Seguridad Física, Uso de Herramientas que Comprometan la Seguridad de las TIC y Uso de los Recursos de la Infraestructura Tecnológica e Información.
Objetivo: Definir el tipo y características de los dispositivos de seguridad contra incidencias que posee el Centro de Computo de la Unidad de Planeación Minero Energética (UPME).
Alcance: Esta norma regula la instalación de dispositivos en el Centro de Cómputo de la entidad.
Descripción: En el Centro de Cómputo de la Unidad de Planeación Minero Energética (UPME), deben existir dispositivos de seguridad que garanticen la detección temprana de incidencias, consideradas como mínimas a controlar. Asimismo, se debe disponer de dispositivos a fin de solventar rápidamente dichas incidencias mínimas a controlar. Los **incidentes** mínimos a contemplar son: ● Interrupción del suministro eléctrico. ● Interrupción de las comunicaciones. ● Interrupción de la refrigeración. ● Detección y prevención de conatos de fuego. ● Detección y prevención de inundaciones.
Acciones de Despliegue e Implantación: ● Implementar las medidas de seguridad necesarias que permitan una rápida respuesta ante cualquier tipo de incidencias. ● Adquirir dispositivos de seguridad para la detección y solución de incidencias.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

NTI019 **Título de la Norma: Seguridad Física –Backups**

Políticas Relacionadas: Acceso a la Información, Administración de la Seguridad de las TIC, Control de Cambios, Continuidad, Cumplimiento de Regulaciones, Documentación y Entrenamiento, Privacidad de la Información, Procesamiento de la Información, Responsabilidad de la Seguridad de las TIC, Responsabilidad del Personal, Seguridad Física y Uso de los Recursos de la Infraestructura Tecnológica e Información.

Objetivo: Definir el control de acceso físico que debe existir en cualquier lugar en que se resguarden dispositivos de almacenamiento de datos.

Alcance: Esta norma define los controles de seguridad física instalados en los lugares donde se guardan dispositivos de almacenamiento de datos y que deberán ser seguidos y analizados por el funcionario asignado de la Oficina de Gestión de la Información de la Unidad de Planeación Minero Energética (UPME).

Descripción: Adicionalmente a las medidas de control de acceso y dispositivos de control de incidencias ya descritas en las normas de seguridad física respectiva, deben adicionarse en los espacios destinados para el resguardo de las copias de seguridad los siguientes aspectos:

- Por el lugar donde se guardan dispositivos de almacenamiento de datos no deben pasar cañerías con fluidos, asimismo deben existir controles de humedad y temperatura, así como detectores de humo y fuego.
- El área destinada al almacenamiento de soportes magnéticos debe ser de uso exclusivo, es decir con ese único fin, para evitar el paso de personas.

Es responsabilidad de la Oficina de Gestión de la Información de la Unidad de Planeación Minero Energética (UPME), el constatar con una periodicidad adecuada que los controles se encuentren correctamente implementados.

Esta norma debe estar incluida en la parte pertinente en el documento de Plan de Contingencia de la Unidad de Planeación Minero Energética (UPME).

Todos los cambios estructurales dentro de los lugares destinados al almacenamiento de datos deben ser informados a la Oficina de Gestión de la Información de la Unidad de Planeación Minero Energética (UPME) a fin de que se evalúe antes de la realización de los mismos las posibles consecuencias sobre la seguridad física establecida.

Acciones de Despliegue e Implantación:

- Adecuar las instalaciones físicas donde se almacenan las copias de respaldo con los mecanismos medioambientales adecuados.
- Probar periódicamente las copias de respaldo.
- Etiquetar las copias de seguridad, de acuerdo a la información que contiene.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

8.2.5. Gestión de incidentes de seguridad de la información.

NTI020 **Título de la Norma: Responsabilidades y procedimientos**
Políticas Relacionadas: Reporte de eventos de seguridad de la información, reporte de debilidades de seguridad de la información, evaluación de eventos de seguridad de la información y decisiones sobre ellos, respuesta a incidentes de seguridad de la información, aprendizaje obtenido de los incidentes de seguridad de la información, recolección de evidencia.
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
Alcance: Esta norma define las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información
Descripción: Para la Gestión de Incidentes se establecen las siguientes etapas: ● **Detección del incidente:** Cada área de la entidad está encargada de notificar al oficial de seguridad sobre los incidentes presentados en su área, con el fin de gestionarlos, mitigando así el impacto que los incidentes generan. ● **Análisis del incidente reportado:** La Unidad de Planeación Minero Energética (UPME) clasifica el tipo de incidente y establece su prioridad (alta, media o baja), con el objetivo de dar prioridad a aquellos incidentes que se cataloguen como críticos dentro de la entidad. ● **Contención o preparación de la solución del incidente:** Acorde con la prioridad en la que se clasifica el incidente se establecen medidas inmediatas con el fin de gestionar el mismo. Estas son medidas de choque para evitar aumentar el impacto, hasta cuando se establece una acción definitiva para mitigar el incidente de forma definitiva. ● **Erradicación del incidente:** Para dar una solución eficaz al incidente, es necesario evaluar y analizar la información de los incidentes similares que se han generan en la entidad, y a su vez se debe tener en cuenta los planes de tratamiento producto de la preparación de la solución del incidente generando así actividades con sus respectivos responsables para erradicar así el incidente generado. ● **Recuperación y seguimiento del incidente:** Se hace seguimiento a la acción emprendida para gestionar el incidente de seguridad en el área específica y se evalúan los resultados de la misma de forma conjunta entre el empleado que reporta el incidente y el oficial de seguridad. Si se considera que la acción realizada gestiono adecuadamente el incidente se procederá a su cierre, si por el contrario no se gestionó de forma adecuada se vuelve a plantear una nueva acción.
Acciones de Despliegue e Implantación: ● Definir, formalizar e implementar el procedimiento para la Gestión de incidentes. ● Formalizar la metodología a usar para detectar, analizar y notificar sobre los incidentes de seguridad. ● Documentar los planes de mejora que llevaron a la solución del incidente.

Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

NTI021 **Título de la Norma: Reporte de eventos de seguridad de la información.**
Políticas Relacionadas: Reporte de eventos de seguridad de la información, reporte de debilidades de seguridad de la información, evaluación de eventos de seguridad de la información y decisiones sobre ellos, respuesta a incidentes de seguridad de la información, aprendizaje obtenido de los incidentes de seguridad de la información, recolección de evidencia.
Objetivo: Definir los canales de gestión para el reporte rápido y oportuno de los eventos de Seguridad de la Información.
Alcance: Esta norma define los canales de gestión apropiados para el reporte de eventos de Seguridad de la Información.
Descripción: La entidad reporta oportunamente la información del incidente a el Oficial de Seguridad: ● Todos los funcionarios, contratistas y terceros de los sistemas y servicios de información notifican y reportan cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios que son utilizados en la entidad. ● La entidad dispone de una función de soporte de respuesta a incidentes que presta soporte y asistencia a los usuarios del sistema de información para el reporte y manejo de los incidentes de seguridad. ● Todos los incidentes de seguridad reportados serán investigados y se les hará seguimiento por parte del Oficial de Seguridad de la Información. ● Todos los incidentes de seguridad serán reportados al CSIRT-Gobierno. En caso que dichos incidentes configuren una violación a la Ley 1273 de 2009 (Ley de Delitos Informáticos en Colombia), estos deberán ser denunciados ante la Fiscalia General de la Nación o a través del CAI Virtual de la Policía Nacional.
Acciones de Despliegue e Implantación: ● Establecer los canales adecuados para el reporte de eventos. ● Definir y divulgar el procedimiento para notificar los eventos de seguridad. ● Formalizar las actividades de soporte y asistencia para la respuesta ante incidentes.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

8.2.6. Gestión de la continuidad del negocio.

NTI022

Título de la Norma: Planificación de la continuidad de la seguridad de la información
Políticas Relacionadas: Planificación de la continuidad de la seguridad de la información, implementación de la continuidad de la seguridad de la información, verificación, revisión y evaluación de la continuidad de la seguridad de la información.
Objetivo: Incluir en los sistemas de gestión de la continuidad del negocio de la entidad, la continuidad de seguridad de la Información.
Alcance: Esta norma define los requisitos para asegurar la continuidad de la seguridad de la información en situaciones adversas.
Descripción: Se establece un plan de continuidad con el fin de restaurar la operación, en un tiempo prudencial después de generada la falla o interrupción, garantizando así la disponibilidad de la información, para tal fin se siguen los siguientes pasos: ● Se hace una evaluación de los procesos más críticos en la Unidad de Planeación Minero Energética (UPME), los cuales afectan de forma directa la operación de la entidad. ● Se establecen e implementan procedimientos para permitir la recuperación y restauración de las operaciones de la entidad, logrando así restablecer la disponibilidad de la información. ● Se identifican y asignan roles y responsabilidades de los funcionarios, contratistas y terceros en el plan de continuidad de la entidad. ● Se hace un monitoreo de la acciones emprendidas y se realiza una revisión para establecer si contribuyeron al restablecimiento de la operación y a la disponibilidad de la información. ● Se deja documentado el resultado de las acciones emprendidas y los resultados de la recuperación y el restablecimiento de la operación de la entidad. ● Se definen e implementan las estrategias de recuperación tecnológica necesarias para garantizar la continuidad de los procesos críticos. ● Se documentan los riesgos que enfrenta el Sector en términos de la probabilidad y el impacto de perder la disponibilidad de recursos tecnológicos críticos, con el objetivo de identificar y determinar la prioridad de los procesos críticos de la entidad. ● Los niveles de recuperación tecnológica mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan, estarán incorporados y definidos en el Plan de Continuidad de Negocio. ● Los dueños de las unidades de negocio son los responsables de mantener documentados y actualizados los procesos a su cargo e informar cualquier cambio al responsable de la gestión del Plan de Continuidad de Negocio.
Acciones de Despliegue e Implantación: ● Definir, formalizar, implementar y divulgar el plan de continuidad de negocio. ● Definir las responsabilidades dentro del plan de continuidad de negocio. ● Evaluar los procesos críticos. ● Monitorear y documentar las acciones emprendidas.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

NTI023

Título de la Norma: Implementación de la continuidad de la seguridad de la información

Políticas Relacionadas: Planificación de la continuidad de la seguridad de la información, implementación de la continuidad de la seguridad de la información, verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Objetivo: Establecer procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información.

Alcance: Esta norma define los controles necesarios para asegurar la continuidad del negocio en la entidad ante situaciones adversas.

Descripción: Para la etapa de implementación del plan de continuidad se debe tener en cuenta los siguientes criterios:

- La Oficina de Gestión de la Información debe hacer pruebas y simulaciones para establecer el nivel de efectividad del plan de continuidad de la entidad, evaluando el tiempo del restablecimiento y la recuperación de la disponibilidad de la información.

Adicionalmente se capacitará por medio de las pruebas a los funcionarios, contratistas y terceros que tienen responsabilidades en el plan de continuidad.

- La entidad debe realizar pruebas de recuperación técnica, asegurando que los sistemas de procesamiento de información puedan restablecerse de manera efectiva.

- La entidad deberá solicitar pruebas de restablecimiento de los servicios prestados por parte de los proveedores de la Unidad de Planeación Minero Energética (UPME), asegurando que los servicios provistos externamente puedan restablecerse de forma adecuada.

- Se deben realizar pruebas completas, para establecer que toda la entidad en su conjunto puede restablecer la operación.

Acciones de Despliegue e Implantación:

- Establecer los procedimientos para asegurar continuidad de la seguridad de la información en la Unidad de Planeación Minero Energética (UPME).
- Definir e implementar los controles necesarios que garanticen la seguridad de la Información.
- Mantener los procesos, procedimientos y controles establecidos.

Fecha de Creación: Octubre de 2015

Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

NTI024

Título de la Norma: Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
Políticas Relacionadas: Planificación de la continuidad de la seguridad de la información, implementación de la continuidad de la seguridad de la información, verificación, revisión y evaluación de la continuidad de la seguridad de la información.
Objetivo: Verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados
Alcance: Esta norma define el monitoreo y seguimiento realizado a los controles de continuidad de la seguridad de la información establecidos e implementados.
Descripción: Los acuerdos de continuidad del negocio deben ser probados periódicamente, utilizando simulaciones realistas (que implican tanto a los usuarios como al personal de la Oficina de Gestión de la Información), para demostrar si el personal es capaz de recuperar la información crítica y los sistemas dentro de escalas de tiempo críticas. La entidad evalúa periódicamente el plan de continuidad y lo actualiza si lo considera necesario.
Acciones de Despliegue e Implantación: ● Evaluar periódicamente el plan de continuidad de negocio. ● Actualizar el plan de continuidad de ser necesario.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021
Responsable de Implantación: Oficial de Seguridad de la Información.

NTI025 **Título de la Norma: Disponibilidad de instalaciones de procesamiento de información.**
Políticas Relacionadas: Planificación de la continuidad de la seguridad de la información, implementación de la continuidad de la seguridad de la información, verificación, revisión y evaluación de la continuidad de la seguridad de la información.
Objetivo: Asegurar la disponibilidad de la seguridad en las instalaciones de procesamiento de información y en los activos de información.
Alcance: Esta norma define los planes y controles que garanticen la seguridad suficiente para cumplir los requisitos de confidencialidad, integridad y disponibilidad.
Descripción: Las instalaciones deben estar listas para garantizar el restablecimiento de la operación cuando sea necesario.
Acciones de Despliegue e Implantación: ● Monitorear la replicación en el Centro de Cómputo. ● Verificar el número de backups exitosos y relanzamiento de los fallidos. ● Implementar las condiciones físicas y ambientales necesarias para asegurar la disponibilidad de la seguridad en las instalaciones.
Fecha de Creación: Octubre de 2015
Fecha de Actualización: Mayo de 2021

Responsable de Implantación: Oficial de Seguridad de la Información.

9. PROCEDIMIENTOS Y REQUISITOS REGULATORIOS ASOCIADOS A LAS POLÍTICAS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN.

ENUNCIADO DE LOS PROCEDIMIENTOS Y REQUISITOS			
Procedimiento Requisito	***Objetivo***	***Política Relacionada***	***Norma Relacionada***
Orientación de la dirección para la gestión de la seguridad de la información	Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	Políticas para la administración del riesgo en la seguridad de la información **- Ref.: ISO/IEC 27001 CL. A.5.1.**	Roles y responsabilidades para la seguridad de la información **- *Ref.: ISO/IEC 27001 CL A.6.1.1.***
Políticas para la seguridad de la información	Definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.	Política de la seguridad de la información **- Ref.: ISO/IEC 27001 CL A.5.1.1**	Roles y responsabilidades para la seguridad de la información **- *Ref.: ISO/IEC 27001 CL A.6.1.1.***
Revisión de las políticas para seguridad de la información	Las políticas para seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continuas.	Revisión de las políticas para la seguridad de la información - **Ref.: ISO/IEC 27001 CL A.5.1.2**	Roles y responsabilidades para la seguridad de la información **- *Ref.: ISO/IEC 27001 CL A.6.1.1.***
Procedimiento para el uso de dispositivos móviles.	Definir guías para la utilización de los dispositivos móviles que contengan información de la Unidad de Planeación Minero Energética (UPME).	Política para los dispositivos móviles **- *Ref.: ISO/IEC 27001* CL A.6.2.1** Organización interna de la seguridad de la información **- *Ref.: ISO/IEC 27001 CL. A.6.1***	Protección del Hardware y Software de Seguridad
Contacto con las autoridades	Se deben mantener contactos apropiados con las autoridades pertinentes.	Contacto con las autoridades **- Ref.: ISO/IEC 27001 CL A.6.1.3**	Roles y responsabilidades para la seguridad de la información **- *Ref.: ISO/IEC 27001 CL A.6.1.1.***
Contacto con grupos de interés especial	Identificar los grupos de interés especiales de profesionales en seguridad de la información.	Gestión de grupos de interés especial **- *Ref.: ISO/IEC 27001 CL A.6.1.4***	Roles y responsabilidades para la seguridad de la información **- *Ref.: ISO/IEC 27001 CL A.6.1.1.***

	Y establecer protocolos de comunicación responsables para el contacto con los grupos de interés.		
Seguridad de la información en la gestión de proyectos	Debe incluirse la seguridad de la información en cualquier tipo de proyecto de la entidad	Seguridad de la información en la gestión de proyectos- **Ref.: ISO/IEC 27001 CL. A. 6.1.5**	Roles y responsabilidades para la seguridad de la información - ***Ref.: ISO/IEC 27001 CL A.6.1.1.***
Teletrabajo	Proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	Teletrabajo - **Ref.: ISO/IEC 27001 CL. A. 6.2.2**	Accesos Remotos
Procedimiento de Selección de Personal	Definir los requisitos y perfiles de los cargos para asegurar que los funcionarios y contratistas son idóneos para las funciones a desempeñar.	Proceso de Selección – ***Ref.: ISO/IEC 27001:2013 CL. A.7.1.1***	Roles y responsabilidades para la seguridad de la información - ***Ref.: ISO/IEC 27001 CL A.6.1.1.***
Términos y condiciones del empleo	Definir acuerdos contractuales con empleados y contratistas que establezcan sus responsabilidades y las de la organización en cuanto a seguridad de la información.	Términos y condiciones del empleo - **Ref.: ISO/IEC 27001 CL. A. 7.1.2**	Roles y responsabilidades para la seguridad de la información - ***Ref.: ISO/IEC 27001 CL A.6.1.1.***
Responsabilidades de la dirección	Exigir a todos los empleados y contratistas la aplicación de la seguridad de la información.	Responsabilidades de la dirección - **Ref.: ISO/IEC 27001 CL. A. 7.2.1**	Roles y responsabilidades para la seguridad de la información - ***Ref.: ISO/IEC 27001 CL A.6.1.1.***
Plan de capacitación en seguridad de la información.	Capacitar a los funcionarios, contratistas y demás terceros sobre el SGSI de la entidad.	Toma de conciencia, educación y formación en la seguridad de la información - ***Ref.: ISO/IEC 27001 CL. A.7.2.2.***	Sensibilización

Proceso disciplinario	Establecer un proceso disciplinario en la entidad para sancionar las faltas de los funcionarios, contratistas y demás terceros por violaciones a la seguridad de la información.	Proceso disciplinario **Ref.: ISO/IEC 27001:2013 CL. A.7.2.3**	Roles y responsabilidades para la seguridad de la información **- *Ref.: ISO/IEC 27001 CL A.6.1.1.***
Terminación de contrato o cambio de responsabilidad en el empleo (Acuerdo de confidencialidad)	Definir los deberes de seguridad de la información de los funcionarios que permanecen después de la terminación o cambio de empleo.	Terminación de contrato o cambio de responsabilidad en el empleo **- *Ref.: ISO/IEC 27001 CL A.7.3.1.***	Roles y responsabilidades para la seguridad de la información **- *Ref.: ISO/IEC 27001 CL A.6.1.1.***
Procedimiento de Gestión de Activos	Identificar, documentar e implementar las reglas para el uso, el seguimiento y control de los activos de información, así como el propietario del inventario de los mismos.	Inventario de activos - ***Ref.: ISO/IEC 27001 CL A.8.1.1*** Propiedad de los activos - ***Ref.: ISO/IEC 27001 CL A.8.1.2*** Uso aceptable de los activos **- Ref.: ISO/IEC 27001 CL A.8.1.3** Devolución de activos - **Ref.: ISO/IEC 27001 CL A.8.1.4**	Administración de Seguridad
Clasificación de la información	Clasificar la información en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Clasificación de la información **- *Ref.: ISO/IEC 27001 CL. A.8.2.1***	Integridad de la Información
Etiquetado de la información	Desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Etiquetado de la información **- Ref.: ISO/IEC 27001 CL. A. 8.2.2**	Integridad de la Información
Manejo de activos	Desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información	Manejo de activos- **Ref.: ISO/IEC 27001 CL. A. 8.2.3**	Administración de Seguridad

	adoptado por la organización.		
Gestión de medios removibles	Gestionar de medios removibles, de acuerdo con el esquema de clasificación adoptado por la entidad.	Gestión de medios removibles - ***Ref.: ISO/IEC 27001 CL. A.8.3.1***	Uso de Equipos Personales
Disposición de los medios de soporte	Disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.	Disposición de los medios de soporte- **Ref.: ISO/IEC 27001 CL. A. 8.3.2**	Uso de Equipos Asignados
Transferencia de medios de soporte físicos	Proteger los medios que contienen información contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Transferencia de medios de soporte físicos- **Ref.: ISO/IEC 27001 CL. A. 8.3.3**	Uso de Equipos Asignados
Administración de accesos.	Establecer, el control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Política de control y Administración de accesos **- Ref.: ISO/IEC 27001 CL. A.9.1.1**	Perfiles de Acceso
Seguridad para Internet.	Determinar los parámetros para el uso y acceso a internet de los funcionarios de la entidad.	Seguridad para Internet. - ***Ref.: ISO/IEC 27001 CL. A.9.1.2***	Seguridad Internet
Seguridad para redes inalámbricas.	Estipular los perfiles de acceso a los usuarios a la red y a los servicios de red.	Seguridad para redes inalámbricas. ***- Ref.: ISO/IEC 27001 CL. A.9.1.2***	Seguridad en Comunicaciones
Administración de cuentas	Asignar y cancelar los derechos de usuarios teniendo en cuenta los registros de los mismos, asegurando la calidad de las contraseñas.	Administración de cuentas ***- Ref.: ISO/IEC 27001 CL. A.9.2.1*** Política de Gestión de contraseñas- ***Ref.: ISO/IEC 27001 CL.*** **A.9.4.3** Suministro de acceso de usuarios **- Ref.: ISO/IEC 27001 CL. A. 9.2.2** Gestión de derechos de acceso privilegiado - **Ref.: ISO/IEC 27001 CL. A. 9.2.3** Gestión de información de autenticación secreta de usuarios- **Ref.: ISO/IEC 27001 CL. A. 9.2.4**	Perfiles de Acceso

		Revisión de los derechos de acceso de usuarios - **Ref.: ISO/IEC 27001 CL. A. 9.2.5** Cancelación o ajuste de los derechos de acceso- **Ref.: ISO/IEC 27001 CL. A. 9.2.6**	
Uso de información de autenticación secreta	Exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Uso de información de autenticación secreta- **Ref.: ISO/IEC 27001 CL. A. 9.3.1**	Perfiles de Acceso
Restricción de acceso a información	Restringir el acceso a la información y a las funciones de los sistemas de las aplicaciones de acuerdo con la política de control de acceso.	Restricción de acceso a información- **Ref.: ISO/IEC 27001 CL. A. 9.4.1**	Perfiles de Acceso
Controles criptográficos	Implementar controles criptográficos para la protección de la información.	Política sobre el uso de controles criptográficos (Protección de la Información) - **Ref.: ISO/IEC 27001 CL. A. 10.1.1**	Perfiles de Acceso
Procedimiento de conexión segura	Controlar mediante un proceso de conexión segura, el acceso a sistemas y aplicaciones.	Procedimiento de conexión segura- **Ref.: ISO/IEC 27001 CL. A. 9.4.2**	Perfiles de Acceso
Uso de programas utilitarios privilegiados	Restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Uso de programas utilitarios privilegiados- **Ref.: ISO/IEC 27001 CL. A. 9.4.4**	Perfiles de Acceso
Control de acceso a códigos fuente de programas	Se debe restringir el acceso a códigos fuente de programas.	Control de acceso a códigos fuente de programas- **Ref.: ISO/IEC 27001 CL. A. 9.4.5**	Perfiles de Acceso
Perímetro de seguridad física	Definir y usar perímetros de seguridad para proteger áreas que contengan información confidencial o crítica.	Perímetro de seguridad física - **Ref.: ISO/IEC 27001 CL. A. 11.1.1**	Seguridad Física
Controles de Accesos Físicos	Proteger mediante controles de acceso apropiados las áreas seguras.	Controles de Accesos Físicos - **Ref.: ISO/IEC 27001 CL. A. 11.1.2**	Seguridad Física

Seguridad de las oficinas, recintos e instalaciones	Aplicar la seguridad física a oficinas, recintos e instalaciones.	Seguridad de las oficinas, recintos e instalaciones - **Ref.: ISO/IEC 27001 CL. A. 11.1.3**	Seguridad Física
Protección contra amenazas externas y ambientales	Diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Protección contra amenazas externas y ambientales- **Ref.: ISO/IEC 27001 CL. A. 11.1.4**	Seguridad Física
Trabajo en áreas seguras	Permitir el desarrollo de las operaciones de la entidad en áreas seguras.	Trabajo en áreas seguras - **Ref.: ISO/IEC 27001 CL. A. 11.1.5**	Seguridad Física
Áreas de despacho y carga	Controlar los puntos de acceso donde pueden entrar personas no autorizadas, para evitar el acceso no autorizado.	Áreas de despacho y carga- **Ref.: ISO/IEC 27001 CL. A. 11.1.6**	Seguridad Física
Ubicación y protección de los equipos	Proteger los equipos para reducir el riesgo de amenaza y peligros del entorno	Ubicación y protección de los equipos - **Ref.: ISO/IEC 27001 CL. A. 11.2.1**	Seguridad Física
Mantenimiento de equipos	Realizar el mantenimiento preventivo a los equipos para garantizar la continuidad del negocio.	Mantenimiento de equipos - **Ref.: ISO/IEC 27001 CL. A. 11.2.4**	Protección del Hardware y Software de Seguridad
Retiro de activos	No retirar los equipos, información o software de su sitio sin autorización previa.	Retiro de activos - **Ref.: ISO/IEC 27001 CL. A. 11.2.5**	Protección del Hardware y Software de Seguridad
Seguridad de equipos y activos fuera del predio	Aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.	Seguridad de equipos y activos fuera del predio- **Ref.: ISO/IEC 27001 CL. A. 11.2.6**	Administración de Seguridad
Disposición segura o reutilización de equipos	Verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobrescrito	Disposición segura o reutilización de equipos- **Ref.: ISO/IEC 27001 CL. A. 11.2.7**	Protección del Hardware y Software de Seguridad
Equipos de usuario desatendido	Asegurarse de que a los equipos desatendidos se les da protección apropiada.	Equipos de usuario desatendido- **Ref.: ISO/IEC 27001 CL. A. 11.2.8**	Protección del Hardware y Software de Seguridad
Gestión para Escritorio limpio y pantalla limpia	Garantizar la confidencialidad de información sensible que se encuentre en el escritorio del equipo asignado, o en el lugar de trabajo de los funcionarios.	Escritorio limpio y pantalla limpia- **Ref.: ISO/IEC 27001 CL. A. 11.2.9**	Administración de Seguridad

Operaciones documentadas	Documentar las operaciones que se realizan en la entidad para estar a disposición de los funcionarios.	Operaciones documentadas **- Ref.: ISO/IEC 27001 CL. A. 12.1.1**	Administración de Seguridad
Gestión de cambios	Controlar los cambios que se hagan en las instalaciones y en los sistemas de procesamiento de información de la entidad.	Gestión de cambios **- Ref.: ISO/IEC 27001 CL. A. 12.1.2**	Gestión de cambios.
Gestión de capacidad	Determinar los requerimientos de capacidad de la entidad que garanticen el desempeño requerido del SGSI.	Gestión de capacidad **- Ref.: ISO/IEC 27001 CL. A. 12.1.3**	Gestión de capacidad
Controles contra códigos maliciosos	Evitar que los códigos maliciosos afecten de los sistemas de información y procesamiento de la entidad.	Controles contra códigos maliciosos**- Ref.: ISO/IEC 27001 CL. A. 12.1.4**	Prevención y Detección de Virus
Respaldo de la información.	Garantizar la disponibilidad de las copias de respaldo de la información sensible de la entidad.	Respaldo de la información. **- Ref.: ISO/IEC 27001 CL. A. 12.3.1**	Copias de Respaldo de Software y Datos de Seguridad
Registro de eventos	Mantener un registro documentado y actualizado de los eventos de seguridad de la información.	Registro de eventos **- Ref.: ISO/IEC 27001 CL. A. 12.4.1**	Registro de Eventos.
Protección de la información de registro	Proteger contra alteración y acceso no autorizado a los registros de la entidad.	Protección de la información de registro **- Ref.: ISO/IEC 27001 CL. A. 12.4.2**	Registro de Eventos.
Registros del administrador y del operador	Monitorear las actividades del administrador y del operador del SGSI.	Registros del administrador y del operador **- Ref.: ISO/IEC 27001 CL. A. 12.4.3**	Registro de Eventos.
Sincronización de relojes	Sincronizar los relojes de todos los sistemas de procesamiento de información con una única fuente de referencia de tiempo.	Sincronización de relojes**- Ref.: ISO/IEC 27001 CL. A. 12.4.4**	Seguridad del Software y Hardware
Instalación de Software en sistemas operativos	Controlar la instalación de software en sistemas operativos, teniendo en	Instalación de Software en sistemas operativos **- Ref.:**	Seguridad del Software y Hardware

	cuenta las reglas para la disposición de software por parte de los usuarios.	**ISO/IEC 27001 CL. A. 12.5.1** Restricciones sobre la instalación de software - **Ref.: ISO/IEC 27001 CL. A. 12.6.2**	
Gestión de las vulnerabilidades técnicas	Evaluar la exposición de la entidad a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Gestión de las vulnerabilidades técnicas - **Ref.: ISO/IEC 27001 CL. A. 12.6.1**	Seguridad del Software y Hardware
Controles sobre auditorías de sistemas de información	Planificar y acordar cuidadosamente las actividades de auditoría, para minimizar las interrupciones en los procesos del negocio.	Controles sobre auditorías de sistemas de información- **Ref.: ISO/IEC 27001 CL. A. 12.7.1**	Roles y responsabilidades para la seguridad de la información **- *Ref.: ISO/IEC 27001 CL A.6.1.1.***
Control de redes	Gestionar las redes para proteger la información en sistemas y aplicaciones.	Control de redes **- Ref.: ISO/IEC 27001 CL. A. 13.1.1**	Seguridad del Software y Hardware
Seguridad de los servicios de red	Identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red.	Seguridad de los servicios de red - **Ref.: ISO/IEC 27001 CL. A. 13.1.2**	Seguridad del Software y Hardware
Separación de redes	Separar las redes de los servicios de información, usuarios y sistemas de Información.	Separación de redes - **Ref.: ISO/IEC 27001 CL. A. 13.1.3**	Seguridad del Software y Hardware
Transferencia de la información	Mantener la seguridad de la información transferida dentro de la entidad y con cualquier entidad externa.	Transferencia de la información **- Ref.: ISO/IEC 27001 CL. A.13.2.1**	Seguridad en Comunicaciones
Acuerdos sobre transferencia de información	Tratar la transferencia segura de información del negocio entre la entidad y las partes externas.	Acuerdos sobre transferencia de información **- Ref.: ISO/IEC 27001 CL. A. 13.2.2**	Seguridad en Comunicaciones
Mensajería electrónica	Proteger adecuadamente la información incluida en la mensajería electrónica.	Mensajería electrónica - **Ref.: ISO/IEC 27001 CL. A.13.2.3**	Seguridad en Comunicaciones

Acuerdos de confidencialidad o de no divulgación	Revisar regularmente los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la Unidad de Planeación Minero Energética (UPME) para la protección de la información.	Acuerdos de confidencialidad o de no divulgación - **Ref.: ISO/IEC 27001 CL. A.13.2.4**	Seguridad en Comunicaciones
Adquisición y Mantenimiento de Sistemas	Asegurar que la seguridad de la información sea una parte integral dentro de la adquisición y mantenimiento de los sistemas de información y operacionales.	Adquisición y Mantenimiento de Sistemas- **Ref.: ISO/IEC 27001 CL. A.14.1**	Seguridad del Software y Hardware
Análisis y especificación de requisitos de seguridad de la información	Establecer los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	Análisis y especificación de requisitos de seguridad de la información- **Ref.: ISO/IEC 27001 CL. A.14.1.1**	Seguridad del Software y Hardware
Seguridad de servicios de las aplicaciones en redes públicas	Proteger la información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas.	Seguridad de servicios de las aplicaciones en redes públicas. - **Ref.: ISO/IEC 27001 CL. A.14.1.2**	Seguridad del Software y Hardware
Protección de transacciones de los servicios de las aplicaciones	Salvaguardar la información involucrada en las transacciones de los servicios de las aplicaciones.	Protección de transacciones de los servicios de las aplicaciones. - **Ref.: ISO/IEC 27001 CL. A.14.1.3**	Seguridad del Software y Hardware
Política de desarrollo seguro	Establecer y aplicar reglas para el desarrollo de software y de sistemas.	Política de desarrollo seguro- **Ref.: ISO/IEC 27001 CL. A. 14.2.1**	Seguridad del Software y Hardware
Procedimientos de control de cambios en sistemas	Controlar los cambios a los sistemas dentro del ciclo de vida de desarrollo mediante el uso de procedimientos formales de control de cambios.	Procedimientos de control de cambios en sistemas- **Ref.: ISO/IEC 27001 CL. A. 14.2.2**	Seguridad del Software y Hardware
Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Revisar los cambios hechos en las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación - **Ref.: ISO/IEC 27001 CL. A.14.2.3**	Seguridad del Software y Hardware
Restricciones en los cambios a los paquetes de software	Limitar a los cambios necesarios a los paquetes de software, y todos los cambios se deben controlar estrictamente.	Restricciones en los cambios a los paquetes de software - **Ref.: ISO/IEC 27001 CL. A.14.2.4**	Seguridad del Software y Hardware

Principios de organización de sistemas seguros	Documentar principios de desarrollo para tener sistemas asegurados durante el ciclo de desarrollo.	Principios de organización de sistemas seguros- **Ref.: ISO/IEC 27001 CL. A. 14.2.5**	Seguridad del Software y Hardware
Ambiente de desarrollo seguro	Proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas.	Ambiente de desarrollo seguro- **Ref.: ISO/IEC 27001 CL. A. 14.2.6**	Seguridad del Software y Hardware
Desarrollo contratado externamente	Supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	Desarrollo contratado externamente **- Ref.: ISO/IEC 27001 CL. A.14.2.7**	Seguridad del Software y Hardware
Pruebas de seguridad de sistemas	Realizar pruebas de funcionalidad de seguridad.	Pruebas de seguridad de sistemas **- Ref.: ISO/IEC 27001 CL. A.14.2.8**	Seguridad del Software y Hardware
Prueba de aceptación de sistemas	Establecer programas de prueba y criterios relacionados para los sistemas de información nuevos, actualizaciones y nuevas versiones.	Prueba de aceptación de sistemas- **Ref.: ISO/IEC 27001 CL. A. 14.2.9**	Software Adquirido
Protección de datos de prueba	Seleccionar, proteger y controlar cuidadosamente los datos de prueba.	Protección de datos de prueba- **Ref.: ISO/IEC 27001 CL. A. 14.3.1**	Administración de Seguridad
Seguridad de la información para las relaciones con proveedores	Acordar los requisitos de seguridad de la información para mitigar los riesgos asociados a las relaciones con proveedores.	Seguridad de la información para las relaciones con proveedores **- Ref.: ISO/IEC 27001 CL. A.15.1.1**	Administración de Seguridad
Tratamiento de la seguridad dentro de los acuerdos con proveedores	Establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la entidad.	Tratamiento de la seguridad dentro de los acuerdos con proveedores **- Ref.: ISO/IEC 27001 CL. A.15.1.2**	Administración de Seguridad
Cadena de suministro de tecnología de información y comunicación	Definir los requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación	Cadena de suministro de tecnología de información y comunicación. - **Ref.: ISO/IEC 27001 CL. A.15.1.3**	Administración de Seguridad

Seguimiento y revisión de los servicios de los proveedores	Auditar con regularidad la prestación de los servicios de los proveedores.	Seguimiento y revisión de los servicios de los proveedores. **Ref.: ISO/IEC 27001 CL. A.15.2.1**	Administración de Seguridad
Gestión de cambios en los servicios de los proveedores	Gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento	Gestión de cambios en los servicios de los proveedores **- Ref.: ISO/IEC 27001 CL. A.15.2.2**	Gestión de cambios
Segregación de funciones, responsabilidades y procedimientos	Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Responsabilidades y procedimientos **- Ref.: ISO/IEC 27001 CL. A.16.1.1**	Gestión de incidentes
Reporte de eventos de seguridad de la información	Informar los eventos de seguridad a través de los canales de gestión apropiados.	Reporte de eventos de seguridad de la información **- Ref.: ISO/IEC 27001 CL. A.16.1.2**	Gestión de incidentes
Informe de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Informe de debilidades de seguridad de la información - **Ref.: ISO/IEC 27001 CL. A. 16.1.3**	Gestión de incidentes
Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Evaluar los eventos de seguridad de la información	Evaluación de eventos de seguridad de la información y decisiones sobre ellos **- Ref.: ISO/IEC 27001 CL. A.16.1.4**	Gestión de incidentes
Respuesta a incidentes de seguridad de la información	Dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Respuesta a incidentes de seguridad de la información- **Ref.: ISO/IEC 27001 CL. A. 16.1.5**	Gestión de incidentes
Aprendizaje obtenido de los incidentes de seguridad de la información	Utilizar el conocimiento adquirido en la resolución de incidentes de seguridad para aplicarlo a eventos futuros.	Aprendizaje obtenido de los incidentes de seguridad de la información **- Ref.: ISO/IEC 27001 CL. A.16.1.6**	Gestión de incidentes

Recolección de evidencia	Identificar, recolectar, adquirir y preservar la información que pueda servir como evidencia.	Recolección de evidencia. - **Ref.: ISO/IEC 27001 CL. A.16.1.7**	Gestión de incidentes
Planificación de la continuidad de la seguridad de la información	Determinar los requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas.	Planificación de la continuidad de la seguridad de la información **- Ref.: ISO/IEC 27001 CL. A.17.1.1**	Gestión de continuidad de Negocio.
Implementación de la continuidad de la seguridad de la información	Asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Implementación de la continuidad de la seguridad de la información **- Ref.: ISO/IEC 27001 CL. A.17.1.2**	Gestión de continuidad de Negocio.
Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Verificar los controles de continuidad de la seguridad de la información establecidos e implementados	Verificación, revisión y evaluación de la continuidad de la seguridad de la información **- Ref.: ISO/IEC 27001 CL. A.17.1.3**	Gestión de continuidad de Negocio.
Disponibilidad de las instalaciones de procesamiento de información	Implementar con redundancia suficiente las instalaciones de procesamiento para cumplir los requisitos de disponibilidad.	Disponibilidad de las instalaciones de procesamiento de información **- Ref.: ISO/IEC 27001 CL. A.17.2.1**	Gestión de continuidad de Negocio.
Protección de registros	Proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada de acuerdo con los requisitos legislativos	Protección de registros - **Ref.: ISO/IEC 27001 CL. A.18.1.3**	Administración de Seguridad
Privacidad y protección de información de datos personales	Asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes	Privacidad y protección de información de datos personales **- Ref.: ISO/IEC 27001 CL. A.18.1.4**	Administración de Seguridad

Reglamentación de controles criptográficos	Usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	Reglamentación de controles criptográficos - **Ref.: ISO/IEC 27001 CL. A. 18.1.5**	Administración de Seguridad
Revisión independiente de la seguridad de la información	Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas organizacionales.	Revisión independiente de la seguridad de la información **- Ref.: ISO/IEC 27001 CL. A.18.2.1**	Administración de Seguridad
Cumplimiento con las políticas y normas de seguridad	Revisar con regularidad el cumplimiento del procesamiento de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas.	Cumplimiento con las políticas y normas de seguridad **- Ref.: ISO/IEC 27001 CL. A.18.2.2**	Administración de Seguridad
Revisión y cumplimiento técnico	Determinar el cumplimiento de las políticas y normas de seguridad de la información	Revisión y cumplimiento técnico **- Ref.: ISO/IEC 27001 CL. A.18.2.3**	Administración de Seguridad