upme
Unidad de Planeación Minero Energética

PLAN DE TRATAMIENTO
DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2016-2018

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El presente plan se elabora con el fin de dar a conocer las acciones e iniciativas que se realizan en el marco de la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información, en el contexto del Modelo Integrado de Planeación y Gestión en especial alineado a las Políticas de Gobierno Digital y Seguridad Digital de la Dimensión Gestión con Valores para Resultados.

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos.

2. OBJETIVO DEL PLAN DE TRATAIMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

2.1. OBJETIVO GENERAL

Establecer las acciones metodológicas para gestionar de manera integral los riesgos de seguridad y privacidad de la información, a partir de su identificación, manejo y seguimiento.

2.2. OBJETIVOS ESPECÍFICOS

- Identificar los riesgos de seguridad y privacidad de la información asociada a los procesos de gestión de la UPME.

- Concientizar a los servidores públicos y proveedores de bienes y servicios de la UPME, sobre la necesidad e importancia de la gestión adecuada de los riesgos de seguridad y privacidad de la información.

- Analizar y valorar los riesgos de seguridad y privacidad de la información con el propósito de establecer los controles y planes de manejo para evitarlos, reducirlos, eliminarlos o mitigarlos.

- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

- Establecer las medidas preventivas y predictivas para impedir la materialización de los riesgos de seguridad y privacidad de la información.

3. ALCANCE

Esta Plan, proporciona la metodología establecida por la Entidad para la administración y gestión de los riesgos a nivel de procesos; orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

4. ÁMBITO DE APLICACIÓN

Los lineamientos definidos en esta Plan, aplican para la gestión de los riesgos de seguridad de la información de la UPME.

5. TÉRMINOS Y DEFINICIONES

Los siguientes son términos y definiciones considerados importantes en el desarrollo del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información:

- **Aceptación de riesgo:** Decisión de asumir un riesgo.

- **Acceso a la información pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados (Art 4,Ley 1712 de 2014)

- **Activo:** Cualquier cosa que tiene valor para la organización.

- **Activo de Información:** En relación con la seguridad y la privacidad de la información, se refiere al activo que contiene información pública que la entidad genera, obtenga, adquiera, transforme o controle en su calidad tal.

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

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo:** Uso sistemático de la información para identificar fuentes y para estimar el riesgo (Guía ISO/IEC 73:2002).

- **Archivo**: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- **Auditoría**: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **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.

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

- **Bases de Datos Personales**: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

- **Comité de Seguridad de la Información:** El Comité de Seguridad de la Información, es un cuerpo integrado por representantes designados por la Alta Dirección con el objetivo de garantizar el apoyo manifiesto a las iniciativas de seguridad. De acuerdo con la Resolución de 208 de 2018 será el Comité de Gestión y Desempeño quien cumpla las veces y las funciones.

- **Ciberseguridad**: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

- **Ciberespacio** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009)

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

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

- **Control:** Las políticas, los procedimientos, las prácticas y la estructura organizativa concebida para mantener los riesgos de seguridad y privacidad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Art 6, Ley 1712 de 2014).

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Art 3, Ley 1581 de 2012).

- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (art 3, Decreto 1377 de 2013).

- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (art 3 literal h Ley 1581 de 2012).

- **Datos Personales Mixtos:** Para efectos de este Plan es la información que contiene datos personales públicos junto con datos privados o sensibles.

- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y a los datos biométricos. (Art 3, Decreto 1377 de 2013).

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

- **Derecho a la intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural. (Jurisprudencia Corte Constitucional).

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

- **Encargado de Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (art 3, Ley 1581 de 2012).

- **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.

- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (art 6, 1712 de 2014).

- **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.

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (art 6, 1712 de 2014).

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

- **Plan de continuidad de negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Protección a la duplicación:** Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se 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 de seguridad de la información será el grupo encargado de realizar el seguimiento y monitoreo al Sistema de Gestión de la Seguridad de la información (SGSI).

- **Responsabilidad Demostrada:** Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- **Responsable del Tratamiento de Datos:** Responsable del Tratamiento de Datos Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

- **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, basada 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 mejorar que permita gestionar el riesgo.

- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (art 3, Ley 1581 de 2012).

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

6. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El éxito de la administración de los riesgos de seguridad de la información depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

- **Alta Dirección**: aprueban las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.

- **Proceso Administración del Sistema Integrado de Gestión**: Genera la metodología para la administración del riesgo de la UPME, coordina, lidera, capacita y asesora en su aplicación.

- **Responsables de los procesos**: Identifican, analizan, evalúan y valoran los riesgos de la UPME (por procesos e institucionales) al menos una vez al año. Si bien los Líderes SGC apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

- **Servidores públicos y contratistas**: ejecutan los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

- **Control Interno**: debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos

7. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La UPME adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, y para ello todos los servidores de la entidad se comprometen a:

1. Conocer y cumplir las normas internas y externas relacionadas con la administración de los riesgos.

2. Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.

3. Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.

4. Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.

5. Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.

6. Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.

7. Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado la Dirección General asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

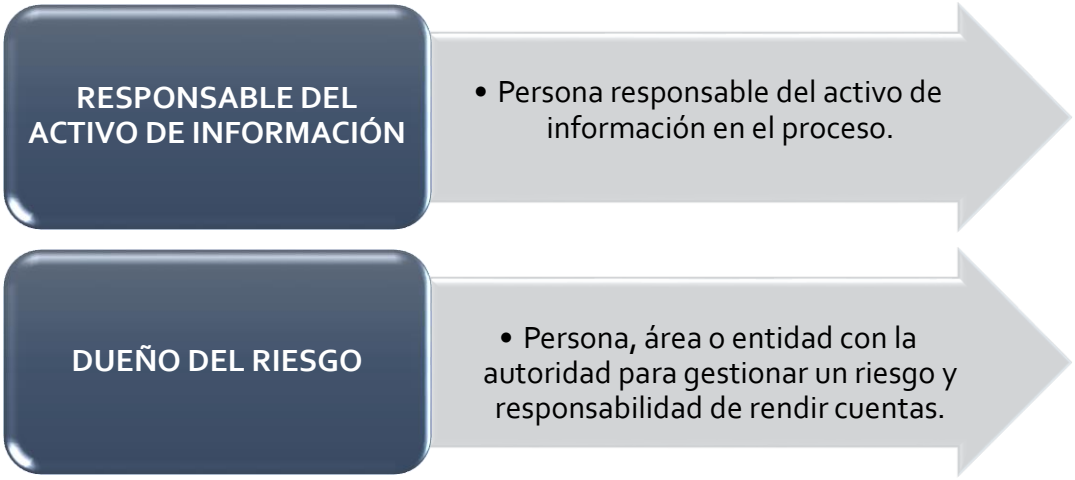
De igual manera, la presente Plan forma parte de la política de administración del riesgo, por cuanto detalla las directrices que deben tenerse en cuenta para la gestión del riesgo en la entidad y que tienen como propósito evitar la materialización del riesgo

8. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

8.1. PROCEDIMIENTO EJECUTADO PARA LA GESTIÓN DE RIESGOS EN LA UPME

8.1.1. Identificación de activos

- Mediante entendimiento de los procesos con los funcionarios participantes de la ejecución de los mismos, se identificaron los activos de información, para posteriormente establecer los riesgos que se encuentran asociados a éstos.
- Se determinaron los responsables y dueños de los riesgos de cada activo de información.



8.1.2. Definición del tipo de activo

Se realizó la siguiente tipificación para los activos de información:

1. Documentos/Información: Datos o Información almacenada o procesada física o electrónicamente. *Ejemplo: Archivos de datos, Información de una base de datos, Contratos, Acuerdos, Documentación del sistema.*

2. Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas. *Ejemplo: Herramientas de Ofimática, Sistemas Manejadores de Bases de Datos, Aplicaciones de Software Específico, Software del Sistema, Herramientas de Desarrollo.*

3. Hardware: se refiere a todas las partes físicas de un sistema informático. *Ejemplo: Equipos de Computación, Equipos de Comunicación, Discos Duros Removibles, Unidades de Backup, Unidades de Almacenamiento.*

4. Servicios: Se consideran tanto los procesos internos, como los externos. *Ejemplo: Gestión Administrativa, Correo Electrónico, Acceso a Internet, Acceso a la Red.*

5. **Personal:** Conocimiento, habilidades y experiencia que posee el personal de una organización. *Ejemplo: Personal de la Organización, Personal Subcontratado, Clientes, Usuarios.*

6. **Intangibles:** Todo aquel activo que no sea posible accederlo físicamente. *Ejemplo: Bases de Datos, Software de Aplicación, Software de Sistema, Correo Electrónico.*

7. Datos/Bases de datos: Datos o Información almacenada o procesada electrónicamente. *Ejemplo: Archivos de datos, Información de una Base de Datos.*

8. Componentes de red: Activos de conectividad entre algunos de los mismos activos de información. *Ejemplo: Hardware, Software y Protocolos.*

9. **Instalaciones:** Activo físico que resguarda los principales activos de información. *Ejemplo Datacenter, Edificios, Instalaciones de TI.*

8.1.3. Criticidad de los activos de Información

Se utilizó una metodología cualitativa para asignar un valor a los activos basado en su importancia. Se dio respuesta a estas 5 preguntas sobre los activos de información:

1. ¿El activo pertenece a terceros?
2. ¿El activo debe estar restringido a un número limitado de usuarios?
3. ¿El activo es muy crítico para las operaciones internas?
4. ¿El activo es muy crítico para el servicio hacia terceros?
5. En caso de que el activo sea utilizado o modificado sin la debida autorización, ¿impactaría negativamente a los sistemas y/o procesos de la UPME y de qué manera? (Leve, Importante, Grave)

Pregunta	Opciones de Respuesta	
	Si	No
¿El activo pertenece a terceros o de clientes?	El activo de información es propiedad de un tercero y es custodiado de forma temporal o permanente por la entidad.	El activo de información es propio de la entidad.
¿El activo debe ser restringido a un número limitado de usuarios?	El activo de información es manejado solamente por un área específica de la entidad.	El activo de información es de conocimiento público o de uso de todos los funcionarios de la entidad.
¿El activo es muy crítico para las operaciones internas?	El activo de información es crítico para la operación ya que compromete la confidencialidad, integridad o disponibilidad de la información de la entidad.	El activo de información no es crítico para la operación ya que no compromete la confidencialidad, integridad o disponibilidad de la información de la entidad.
¿El activo es muy crítico para el	La gestión del activo de información afecta de manera directa o	La gestión del activo de información afecta de manera indirecta o poco

Pregunta	Opciones de Respuesta	
	Si	No
servicio hacia terceros?	importante el servicio que se presta hacia terceros.	representativa el servicio que se presta hacia terceros.

Tabla 1. Criterios para la calificación del nivel de criticidad del activo de información.

En caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactarían negativamente a los sistemas y/o procesos de la UPME de manera:

Impacto	Criterio de evaluación
Leve	La modificación no autorizada del activo de información afectaría de forma moderada la seguridad de la información.
Importante	La modificación no autorizada del activo de información afectaría de manera representativa la seguridad de la información.
Grave	La modificación no autorizada del activo de información afectaría de manera severa la seguridad de la información.

Tabla 2: Nivel de Impacto para la calificación del nivel de criticidad del activo de información

- Se identificó la criticidad de la posible afectación de cada activo de información identificado en cada proceso, mediante la metodología para evaluar los activos, descrita anteriormente.

8.1.4. Clasificación de los activos de información

Se clasifican los activos de acuerdo a la política de clasificación de la información definida por la UPME:
Para clasificar la información, se tomarán en cuenta los siguientes niveles de acuerdo a la Ley 1712 en su Artículo 6:

- **Información Pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en al artículo 18 de esta ley.

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento

de totalidad por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

8.1.5. Identificación y análisis de los riesgos

Se identificaron las amenazas por medio del entendimiento de los procesos y análisis mediante equipos de trabajo con los responsables de los activos, teniendo en cuenta el conocimiento de las actividades de la entidad y el comportamiento histórico de los procesos. Las amenazas se contextualizaron de acuerdo a las posibles vulnerabilidades y efectos del riesgo a las que puede estar expuesto el activo y con base a la forma en que una amenaza podría a llegar a explotar una vulnerabilidad de forma intencional o no y ocasionar daños (Riesgo), afectando en alguna medida la confidencialidad, integridad o disponibilidad de la información.

8.1.6. Valoración de los riesgos en los procesos de la UPME

Se utilizó una metodología cualitativa con un equipo de expertos, principalmente con funcionarios del área bajo análisis. Para valorar los riesgos de Seguridad de la Información se determinó la probabilidad de ocurrencia para cada riesgo teniendo en cuenta los siguientes criterios de valoración:

Valoración	*Valor Asignado*	*Criterio*
Raro	1	Evento que puede ocurrir solo en circunstancias excepcionales.
Improbable	2	El evento difícilmente puede ocurrir en algún momento.
Posible	3	El evento podría ocurrir en algún momento.
Probable	4	El evento que probablemente ocurrirá en la mayoría de las circunstancias.
Muy probable	5	Se espera que el evento ocurra en la mayoría de las circunstancias.

Tabla 3: Criterios para la valoración de los riesgos asociados a activo de Información

a) Se elaboró 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.
Menor	2	Afectación leve de la confidencialidad, integridad y disponibilidad de la información.

Valoración	Valor Asignado	Criterio
Moderado	3	Afectación moderada de la confidencialidad, integridad y disponibilidad de la información.
Mayor	4	Afectación grave de la confidencialidad, integridad y disponibilidad de la información.
Catastrófico	5	Afectación muy grave de la confidencialidad, integridad y disponibilidad de la información.

Tabla 4: Parámetros para la valoración del impacto de los riesgos asociados a activo de Información

Se establecieron los niveles de riesgos (combinación del nivel de probabilidad e impacto) teniendo una clasificación basada en la probabilidad de ocurrencia y el impacto evaluados con anterioridad:

Zona de Riesgo	Valor Asignado	Acción requerida
Riesgo Extremo	Mayor o igual a 15	Requiere acciones inmediatas para evitar la materialización del riesgo.
Riesgo Alto	Mayor o igual a 10 y menor de 15	Requiere acciones rápidas para disminuir el riesgo a niveles inferiores del actual.
Riesgo Medio	Mayor o igual a 5 y menor de 10	Requiere acciones diligentes para disminuir el riesgo a niveles inferiores del actual.
Riesgo Bajo	Menor de 5.	Requiere acciones preventivas para disminuir el riesgo a niveles inferiores del actual.

Tabla 5: Zona de riesgo

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

La Evaluación de los controles se realizó cuando se estableció 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 realizó de la siguiente manera:

a. Mediante entrevistas con los dueños de los procesos se realizó la identificación de los controles relacionados a cada uno de los riesgos establecidos. Fue necesario determinar si el control existe y de no ser así, se dejó el registro.

b. Si los controles existen, se realizó la descripción del mismo y se hizo la asociación con los controles del Anexo A de la norma ISO 27001:2013 correspondientes, se procedió a realizar la calificación de cada uno teniendo

como criterio las cualidades y características. Se tienen como cualidades de los controles las siguientes:

c. Las características se resumen en lo siguiente:

CARACTERÍSTICAS	DESCRIPCIÓN
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 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	Período 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	Determina si el control es: adecuado/no adecuado.
Responsabilidad	Determina si la responsabilidad está: definida/no definida.
Cargo	Nombre del cargo que ejecuta el control.
Tipo de control	Control: detectivo / preventivo / correctivo.
Importancia sobre la mitigación del riesgo	Percepción del dueño del riesgo del activo: establece si este control es relevante para mitigar el riesgo (importante/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 6: Características para la valoración 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%	0,9	¿El control Existe?
	0,1	Actividades que componen el control
CARACTERISTICAS		
80%	0,15	Categoría del Control
	0,1	Naturaleza
	0,025	Funcionalidad de la Naturaleza
	0,1	Documentación
	0,1	Complejidad
	0,025	Funcionalidad de la complejidad
	0,1	Responsabilidad
	0,15	Tipo de control
	0,05	Importancia sobre la mitigación del riesgo
	0,1	Disminuye la probabilidad
	0,1	Disminuye el impacto

Tabla 7: Ponderación de las cualidades y características para la valoración 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 que sean menores a 0,7 se consideran “Controles no Efectivos”, si es mayor o igual a 0,7 y menor a 1,05 se considera “Poco Efectivo”, si es mayor o igual a 1,05 y menor a 1,4 se considera “Efectivo” y si es mayor o igual a 1,4 se considera “Muy efectivo”.

CRITERIOS	DEFINICIÓN
Muy Efectivo	Se cuenta con controles eficientes y robustos que garantizan la gestión del riesgo.
Efectivo	Los controles existentes brindan cierto nivel de seguridad razonable para la gestión del riesgo.
Poco Efectivo	Los controles existentes no son suficientes para la gestión efectiva del riesgo.

CRITERIOS	DEFINICIÓN
Controles no efectivos	Los controles existentes evidencian la falta de gestión del riesgo.

Tabla 8: Nivel de Efectividad de los controles

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.

i. El desplazamiento de los riesgos tienen en cuenta la matriz de referencia (tabla 6) 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 y en impacto es 2, podría tener tres controles asociados, donde dos de ellos disminuyen 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).

Promedio	Valor Actual (Impacto / Probabilidad)				
	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	0	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 9: Unidades de desplazamiento del riesgo tras la evaluación de controles

8.1.8. Establecer un plan de tratamiento de cada uno de los riesgos asociados a los activos de información de la UPME.

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

a) Si el riesgo se encuentra en una zona de aceptación o apetito de riesgo según lo establecido en la política para la aceptación del riesgo.
b) Si es susceptible de ser tratado a través de la implantación de un nuevo control o fortaleciendo los ya existentes (esto podría lograrse a través de una disminución en los niveles de impacto y/o de la probabilidad).
c) Si la decisión es aceptar ese nivel de riesgo, independiente donde se encuentre ubicado en el mapa de riesgos y la afectación que pueda tener para Confidencialidad, Integridad y Disponibilidad de la información, se contemplará la aplicación de controles complementarios.
d) Si se decide ignorar, es posible determinar la reiniciación del análisis.
e) Si la decisión es transferir, se sugieren realizar el análisis de costo beneficio correspondiente.

8.1.9. Continuidad de los planes de tratamiento de los riesgos asociados a los activos de información de la UPME

Se debe definir un plan de acción para el tratamiento de los riesgos de seguridad de la información.

La UPME, debe tener claro al momento de decidir implementar nuevos controles o transferir los riesgos, se pueden generar nuevos riesgos que afecten la seguridad de la información. Por tal razón se debe iniciar un ciclo completo de análisis, evaluación y tratamiento (si da lugar) de riesgos a los mismos procesos allí incluidos.

La UPME, debe realizar una revisión con una frecuencia definida o cuando haya lugar, donde apuntando a la gestión del sistema, a su adecuado seguimiento y a la mejora continua se reiniciará el análisis de la gestión de riesgos con base en el estado identificado.

.

8.2. ACCIONES DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 2016-2018

Las iniciativas para el periodo 2016-2018 impulsan la implementación adecuada del Sistema de Gestión de Seguridad de la Información en la entidad, acciones enmarcadas en la identificación, análisis y valoración de los riesgos y acciones de tratamiento necesarias en implementarse para su ejecución.

Dentro de las principales iniciativas para el año en mención, se encuentran las siguientes:

ACTIVIDAD	DESCRIPCION	RESPONSABLE	META	PRODUCTO	FECHA	
					INICIO	FIN
Planificación de la gestión de riesgos de Seguridad Digital	El propósito de la planificación de la gestión del riesgo de seguridad digital es esencial, pues es el punto de partida para el desarrollo de la GRSD, la cual se centra en la ejecución de una serie de actividades previas y orienta a las entidades para que establezcan o formalicen: • Compromiso de la alta dirección • Establecimiento del contexto organizacional en el entorno digital. • Identificación de partes interesadas y procesos donde se desarrollará la gestión de seguridad digital. • Desarrollo de una política de gestión de riesgo o la armonización con una política de seguridad de la información existente. • Definición de roles y responsabilidades para la gestión de riesgos de seguridad digital. • Recursos necesarios para la gestión de riesgos de seguridad digital. • Criterios para la gestión del riesgo de seguridad digital.	Director General Comité MPGI Oficial de Seguridad Oficial de Riesgos	60%	Implementación SGSI en la UPME (C-006-2015) Resolución 304 de 2016 C-019-2016 (BK) 210-2016-114(Nes)	27/07/2015 29/09/2016 18/11/2016	31/12/2015 29/11/2016 18/12/2016

ACTIVIDAD	DESCRIPCION	RESPONSABLE	META	PRODUCTO	FECHA	
					INICIO	FIN
Ejecución de la gestión de riesgos de seguridad digital (GRSD)	Esta fase contempla las actividades para la ejecución de la gestión de riesgos de seguridad digital. Cada una de las acciones define sus salidas o entregables, las cuales se ilustran a continuación: • Identificación de los activos de información. • Identificación de riesgos inherentes de seguridad digital. • Valoración de riesgos inherentes de seguridad digital. • Identificación y evaluación de controles. • Tratamiento de los riesgos de seguridad digital.	Oficial de Seguridad Oficial de Riesgos	60%	Implementación SGSI en la UPME (C-006-2015) Resolución 304 de 2016 210-2017-145(AV)	27/07/2016 06/12/2017	31/12/2016 12/12/2017
Monitoreo, revisión y reporte de la gestión del riesgo de seguridad digital.	Revisión periódica usando diferentes estrategias como las descritas a continuación: • Revisión por la alta dirección. • Auditorías internas y externas. • Medición del desempeño. • Rendición de cuentas.	Director General Comité MPGI Oficial de Seguridad Oficial de Riesgos	30%	Informe final con los hallazgos y las recomendaciones respectivas: 200-2016-065(Nov) 210-2016-114(Nex) 200-2017-096(EH) 210-2017-145(AV	27/07/2016 18/11/2016 01/09/2017 06/12/2017	27/10//2016 18/12/2016 01/11/2017 12/12/2017
Mejora para la gestión del riesgo de seguridad digital.	Esto tiene como fin preservar la confidencialidad, integridad y disponibilidad de los activos de información y propender por minimizar los impactos económico, social y ambiental que se puedan derivar de estos riesgos. • Comunicación y consulta. • Comunicación y capacitación de la aplicación del modelo de gestión de riesgos de seguridad digital (GRSD).	Oficial de Seguridad Oficial de Riesgos				

9. SEGUIMIENTO Y EVALUACIÓN AL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Para el aseguramiento de la ejecución del Plan de Tratamiento de Riesgos seguridad y privacidad de la información en el marco del Plan Estratégico Institucional, se utilizaran los instrumentos que se han definido así:

- Seguimiento a través del Plan de Acción de la UPME de:

❖ Las acciones planificadas en el presente plan, del tratamiento de los riesgos sobre los activos de información incluidos como parte de la planeación e implementación del SGSI de la UPME.
❖ Las actividades planificadas para cada vigencia respecto a la ejecución de los ejercicios de Hacking Ético en la infraestructura de los servidores de la UPME.

- Seguimiento al Plan de Mejoramiento Institucional producto de:
❖ Auditorías Internas y Externas al SGSI.
❖ Recomendaciones u oportunidades de mejora tras las revisiones de los entes de control.

- Seguimiento en los proyectos de inversión de las actividades asociados con la seguridad y privacidad de la información.

- Seguimiento y evaluación de los indicadores de gestión del Sistema de Gestión de Seguridad de la Información.

10. CONTROL DE CAMBIOS

Fecha	Versión	No. Comité de Gestión y Desempeño de Aprobación	Observación o Motivo del Cambio
31/07/2018	1	Comité. No 3 del 30/07/2018	Aprobación y publicación de este documento.