INFORME DE AUDITORÍA INTERNA AL PROCESO DE GESTIÓN TICs – MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

Informe de Auditoría	Auditoría Interna al proceso Gestión TICs – Modelo de Seguridad y Privacidad de la Información (MSPI)
Líder del proceso	Gladys Rubiela Rodríguez Martínez Jefe Oficina de Gestión de la Información
Elaborado por:	Leonel Mauricio Velandia Gómez Profesional Especializado
Revisado y Aprobado por:	Ingrid Cecilia Espinosa Sánchez Asesora de Control Interno (e)
Fecha del Informe:	2023/12/22

TABLA DE CONTENIDO

1. OBJETIVO

Evaluar los mecanismos de control establecidos por el proceso para dar cumplimiento al objetivo y al Modelo de Seguridad y Privacidad de la Información (MSPI).

2. ALCANCE

El ejercicio de auditoria corresponde a la gestión adelantada desde el 01 de enero de 2022 hasta el 31 de octubre de 2023.

3. METODOLOGÍA UTILIZADA

El programa anual de auditoría interna para la vigencia 2023, aprobado en Comité Institucional de Coordinación de Control Interno el día 12 de enero de 2023 en sesión virtual estableció la ejecución de auditoria al proceso Gestión TICs – Modelo de Seguridad y Privacidad de la Información en el mes de noviembre.

Dando cumplimiento a lo mencionado, se realiza reunión de apertura de la auditoria el día 30 de noviembre de 2023, en la cual se realizó la formalización del plan de auditoría, informando de esta manera el objetivo, alcance, criterios de la auditoría y las actividades que se realizarían durante este ejercicio, y confirmando la entrega de información solicitada el 15 de noviembre de 2023 por el anterior auditor, ya que corresponde a la base del inicio de la evaluación de la implementación del modelo de seguridad y privacidad de la información, la cual fue entregada el 28 de noviembre de 2023.

Con el fin de establecer un grado de madurez promedio de los procesos, se aplicó una calificación definida dentro de un rango, de acuerdo con el número de Observaciones y Hallazgos, tal como se expresa en la siguiente Tabla:

Grado de Madurez	Calificación	Hallazgos	Observaciones
Alto	Mayor a 4.5	0-1	1-2
Medio	Entre 3.5 – 4.5	2-3	3-5
Bajo	Menor 3.5	4 ó más	6 ó más

Tabla 1. Cálculo del Grado de Madurez Promedio del Procedimiento Auditado.

4. ASPECTOS RELEVANTES DE LA AUDITORÍA

El programa anual de auditoría interna para la vigencia 2023, aprobado en Comité Institucional de Coordinación de Control Interno el día 12 de enero de 2023 en sesión virtual estableció la ejecución de auditoria al proceso Gestión TICs – Modelo de Seguridad y Privacidad de la Información en el mes de noviembre. Dando cumplimiento a lo mencionado, la asesoría de Control Interno asignó al auditor Alexander Bueno Herrera – Profesional Especializado código 2028 grado 17, sin embargo, con el fin de identificar un posible conflicto de intereses, se realiza solicitud a la jefatura de la Oficina de Gestión de la Información mediante memorando 20231000025893 de fecha 09 de agosto de 2023 en la que informe si la funcionaria Sandra Patricia Zambrano Tapia – Profesional Especializado código 2028 grado 17 tiene asignadas funciones relacionadas con el objetivo y alcance de la auditoría, esto con el fin de determinar si se debe realizar cambio de auditor.

Teniendo en cuenta que no se recibió respuesta dentro del siguiente mes, se mantiene la decisión de asignar al auditor mencionado para la ejecución de la auditoría, por tanto,

dando cumplimiento al programa anual de auditorías para la vigencia 2023, se envía correo a la jefatura de la oficina de gestión de información el día 15 de noviembre de 2023, en el cual se realiza solicitud de información, se informa el plan de auditoría y se programa reunión de apertura para el 17 de noviembre de 2023.

Así las cosas, el día 16 de noviembre siendo las 7:09pm se recibe correo electrónico del jefe encargado de la oficina de gestión de información, quien, dando respuesta al memorando del 09 de agosto de 2023, manifiesta el posible conflicto de intereses así:

> *"Como Jefe(E) de la Oficina de Gestión de la Información y en relación a la auditoría que se iniciaría el día de mañana 17 de noviembre frente al proceso de Gestión de TIC´s – Modelo de Seguridad y Privacidad de la Información MSPI, y dado que la funcionaria Sandra Patricia Zambrano Tapia quien labora en la Oficina de Gestión de la Información cuenta dentro de su manual de funciones numeral 11 "Aplicar las políticas en materia de seguridad de la información de la Entidad de conformidad con los lineamientos de políticas vigentes" y a pesar que su labor dentro de la oficina no contempla actividades específicas asociadas al modelo de seguridad y privacidad de la información MSPI, puede existir un aparente conflicto de interés basado en consideraciones expresas de pertenecer a la oficina propietaria del proceso de Gestión TICS."*

Conforme lo anterior, durante la reunión de apertura el día 17 de noviembre de 2023 se solicita por parte del auditado el cambio de auditor, para lo cual la Asesora de Control Interno (e), pesé a considerar que no existe conflicto de intereses por parte del auditor inicialmente designado, toma la decisión de aceptar la solicitud del cambio de auditor y revisar al interior del equipo de Control Interno quien podría realizar la auditoría conforme la disponibilidad. De esta manera, fue asignado como auditor Leonel Mauricio Velandia Gómez – profesional especializado código 2028 grado 18 el día 17 de noviembre de 2023, quien da inició a la planeación de la auditoría, y el día 27 de noviembre de 2023 procede a enviar citación para reunión de apertura, la cual se efectuó el 30 de noviembre de 2023, presentado de esta manera un nuevo plan de auditoría y manteniendo la solicitud de información ya realizada, la cual fue la base del inicio de la evaluación de la implementación del modelo de seguridad y privacidad de la información.

4.1. Criterios de Auditoría

- Constitución Política de la República de Colombia.
- Ley 87 de 1993. Por medio de la cual se establecen normas para el ejercicio del Control Interno en las entidades y organismos del Estado.
- Decreto 1258 de 2013. Por el cual se modifica la estructura de la Unidad de Planeación Minero Energética - UPME.
- Decreto 1259 de 2013. Por el cual se modifica la planta de personal de la Unidad de Planeación Minero Energética - UPME y se dictan otras disposiciones.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Resolución de MinTIC 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se

definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- Decreto 1073 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Administrativo de Minas y Energía.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1083 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
- Decreto 415 de 2016. Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
- Decreto 767 de 2022. 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 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Modelo Integrado de Planeación y Gestión.
- Modelo de Seguridad y Privacidad de la Información – MSPI
- Mapa de Riesgos.
- Planes de Mejoramiento de auditorías anteriores.
- Demás normatividad vigente aplicable.

5. FORTALEZAS Y DEBILIDADES

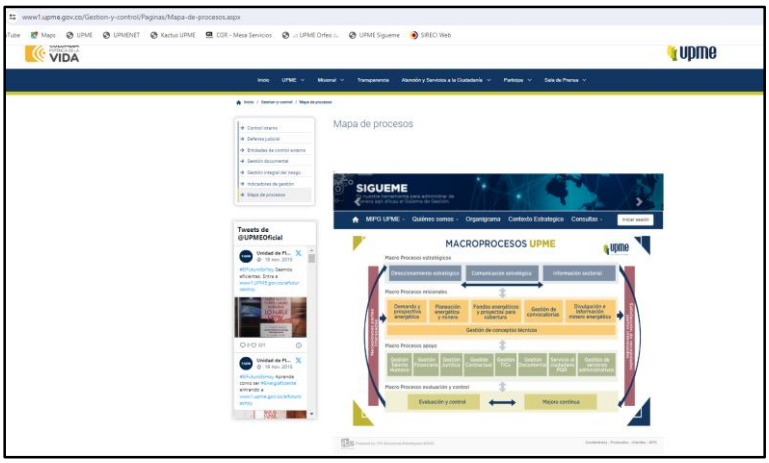
5.1. Fortalezas

No se han identificado fortalezas en la evaluación realizada a la documentación requerida por el Modelo de Seguridad y Privacidad de la Información para su implementación, sustentada en las oportunidades de mejora y hallazgos del presente informe.

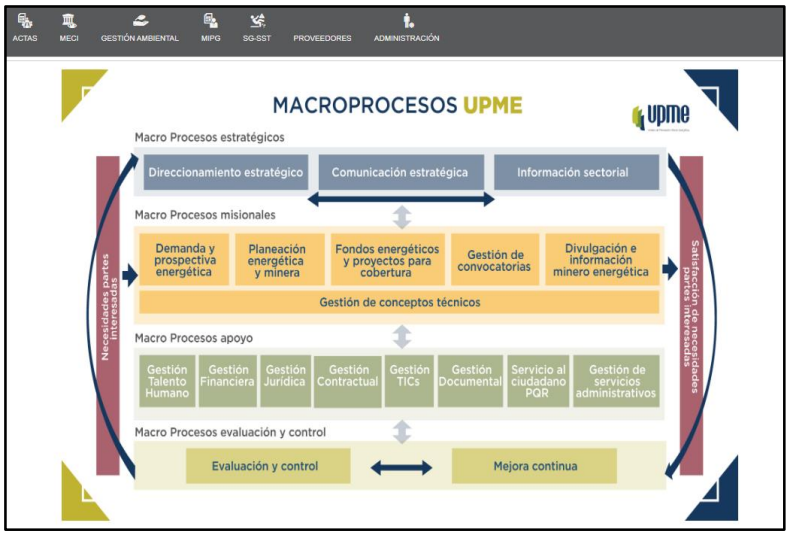
5.2. Debilidades

- Suministro de información y/o respuestas a las observaciones no fueron oportunas o no se realizaron, lo que dificulto la labor de auditoría al Modelo de Seguridad y Privacidad de la Información.

- En el marco del modelo de operación por procesos de la entidad se determina el alcance del Modelo de Seguridad y Privacidad de la Información para un total de veintiún (21) procesos, sin embargo, en el mapa de procesos de la entidad disponible en el sitio web y en el Sistema de Gestión Único Estratégico de Mejoramiento - SIGUEME, se puede establecer que el modelo de operación por procesos de la entidad cuenta con diecinueve (19) procesos, por lo que se puede establecer que no hay claridad frente al modelo de operación por procesos de la Unidad de Planeación Minero Energética – UPME.



Tomado de Sitio Web: https://www1.upme.gov.co/Gestion-y-control/Paginas/Mapa-de-procesos.aspx



Tomado de la página de inicio del Sistema de Gestión Único Estratégico de Mejoramiento – SIGUEME.

- En términos generales se puede establecer que hay debilidades en la documentación que el Modelo de Seguridad y Privacidad de la Información establece como salidas o resultados de cada una de las fases de su implementación.

6. RESULTADOS DE AUDITORÍA

6.1. Oportunidades de Mejora

6.1.1. Actualización del documento Modelo Operativo de Seguridad Digital, ya que algunas de las resoluciones mencionadas en el documento se encuentran derogadas, y algunos de los hallazgos presentados en el presente informe de auditoría, no cumplen con los requerimientos del Modelo de Seguridad y Privacidad de la Información en lo relacionado con la conformación del Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno, así como la delegación por parte del director general de la UPME del Oficial de Seguridad de la Información.

6.1.2. Actualizar la "Guía Operacional de Gestión de Activos de Información", para el cual se tienen las siguientes observaciones:

- Salvo la definición de que es un activo de información, no se establecen los tipos de activos de información, como por el ejemplo: Los datos creados por la entidad, el hardware y software, los servicios utilizados para transmisión, recepción y control de información, las herramientas o utilidades para el desarrollo y soporte de los sistemas de información e incluso algunas personas.

- No se evidencia en el documento la explicación de cómo realizar la clasificación de la información conforme los tres principios de la seguridad de la información (confidencialidad, integridad y disponibilidad).

- No se establece la periodicidad para realizar la actualización de los inventarios y la clasificación por parte de los propietarios y custodios de los activos, conforme lo establece el numeral 7.3.1. Identificación de activos de información e infraestructura crítica, ya que indica que debe hacerse de forma periódica o toda vez que exista un cambio en el proceso.

  Así las cosas, al ser un documento que debe orientar a los líderes de los procesos y los colaboradores de la entidad en general para una adecuada identificación y clasificación de activos de información, debe ser un documento que realmente de claridad sobre los tipos de activos que se pueden identificar, como se realiza la clasificación de la información, la periodicidad para realizar la revisión y/o actualización de los activos de información, entre otras. De igual manera, debería contemplar información sobre el adecuado diligenciamiento del formato de activos de información, en cada una de las columnas que este documento solicita.

6.1.3. Unificar la metodología para la identificación de los activos de información, y la publicación de los que correspondan a datos abiertos o sean información pública, incluyendo activos tales como Hardware, Software, información física y digital, recursos humanos (contratista y Planta), servicios, entre otros, los cuales son activos de información identificados bajo el modelo MSPI.

6.1.4. Actualizar el "Procedimiento de Gestión de Riesgos de Seguridad Digital" conforme lo establece la "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6" expedida en noviembre de 2022.

6.1.5. Fortalecer la formulación de los planes de comunicación asegurando que se contemplan los lineamientos y el propósito que establece el numeral 7.4.2. del Documento Maestro de Seguridad y Privacidad de la Información (página 33).

6.1.6. Teniendo en cuenta que el Modelo de Seguridad y Privacidad de la Información no solo tiene relación con temas tecnológicos, sino que es un modelo transversal a la entidad que busca la implementación de controles de seguridad tanto físicos como lógicos para asegurar los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno, en este caso de la Unidad de Planeación Minero Energética - UPME, mediante una gestión eficaz, eficiente y efectiva de los activos de información, la infraestructura, los riesgos e incidentes de seguridad y privacidad de la información con el fin de evitar la afectación en la prestación de los servicios de la entidad y su modelo de operación por procesos, se deben realizar las acciones correspondiente para que se lidere de manera transversal la implementación del modelo desde el proceso direccionamiento estratégico, acorde con los lineamientos de MSPI que requiere la intervención de los comités institucional de Gestión y Desempeño así como el de Coordinación de Control Interno en cada una de sus fases.

6.2. Hallazgos

6.2.1. Conforme Acta No. 001 de 12 de octubre de 2016 del Comité de Seguridad de la Información se aprobó por unanimidad la designación del Oficial de Seguridad de la Información al señor Luis Antonio Hurtado por parte de este comité, pesé a que el artículo 5 de la resolución 304 de 2016 (25-05-2016) establece que es el Director General de la entidad quien debe hacer la designación de este Oficial. Por otra parte, se pudo establecer que el señor Hurtado pertenece a la Oficina de Gestión de Información (la cual hace las veces de Oficina o Dirección de Tecnología en la Entidad) y el documento maestro del Modelo de Seguridad de la Información Versión 4 de 28-10-2021 establece que este Oficial de Seguridad "deberá depender de un área estratégica que no sea la Oficina o Dirección de Tecnología (se recomienda el despacho de nominador)", incumpliendo lo establecido en el numeral 7.2.3. Roles y Responsabilidades – Lineamiento, del Documento Maestro del Modelo de Seguridad y Privacidad de la Información (página 28) el cual establece "Se debe delegar a un responsable de la seguridad y privacidad de la información" y "… si el cargo no existe en la entidad deberá ser delegado por acto administrativo y deberá depender de un área estratégica que no sea la Oficina o Dirección de Tecnología (se recomienda el despacho de nominador)," y el artículo 5 de la resolución 304 de 2016 que establece "Oficial de Seguridad de la Información. Esta Labor será ejercida por un Profesional Especializado designado por el Director General, y quien tendrá las funciones como

Oficial de Seguridad de la Información de la Entidad. Dependerá funcional y administrativamente de la Oficina o Subdirección que el Director General designe".

6.2.2. No se ha incluido al responsable de la seguridad y privacidad de la información (Oficial de Seguridad de la Información) como miembro con voz y voto en el Comité Institucional de Gestión y Desempeño, tal como se puede evidenciar en el artículo 3 de la resolución 277 de 2020 "Por la cual se crea el Comité Institucional de Gestión y Desempeño de la Unidad de Planeación Minero Energética, se adopta Sistema de Gestión bajo el Modelo Integrado de Planeación y Gestión y se dictan otras disposiciones", incumpliendo lo establecido en el **numeral 7.2.3. Roles y Responsabilidades – Lineamiento, del Documento Maestro del Modelo de Seguridad y Privacidad de la Información (página 28)** el cual establece *"… de igual manera la persona designada deberá ser incluida como miembro del comité de gestión institucional con voz y voto…".*

6.2.3. No se ha incluido al responsable de la seguridad y privacidad de la información (Oficial de Seguridad de la Información) como miembro con voz sin voto en el Comité Institucional de Coordinación de Control Interno, tal como se puede evidenciar en el artículo 1 de la resolución 693 de 2017 "Por medio de la cual se conforma el Comité Institucional de Coordinación de Control Interno de la Unidad de Planeación Minero Energética - UPME", incumpliendo lo establecido en el **numeral 7.2.3. Roles y Responsabilidades – Lineamiento, del Documento Maestro del Modelo de Seguridad y Privacidad de la Información (página 28)** el cual establece *""… de igual manera la persona designada deberá ser incluida como miembro del comité de gestión institucional con voz y voto … y en el comité de control interno con voz".*

6.2.4. El documento P-TI-006 "Procedimiento de Gestión de Riesgos de Seguridad Digital" creado el 19 de septiembre de 2022 y vigente en el Sistema de Gestión Único Estratégico de Mejoramiento – SIGUEME a partir del 20 de septiembre de 2020, no fue aprobado por el Comité Institucional de Coordinación de Control Interno, como se pudo establecer con las actas del mencionado comité publicadas en el sitio web de la entidad en la URL https://www1.upme.gov.co/Gestion-y-control/Paginas/Actas-comite-institucional.aspx, incumpliendo **el numeral 7.3.2. Valoración de los riesgos de seguridad de la información - Salidas del Documento Maestro del Modelo de Seguridad y Privacidad de la Información (página 30)** el cual establece *"Procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité de coordinación de control interno"*.

6.2.5. No fue presentada al auditor la declaración de aplicabilidad del plan de tratamiento de los riesgos de la seguridad de la información, por tanto, no se puede establecer que la entidad cuenta con dicha declaración de aplicabilidad debidamente aceptada y aprobada por el Comité Institucional de Gestión y Desempeño y que contenga los controles necesarios, el estado de implementación de dichos controles y la justificación de las posibles exclusiones, incumpliendo lo establecido en **el numeral 7.3.3. Plan de Tratamiento de los riesgos de seguridad de la información -**

Lineamiento (página 31) del documento maestro del Modelo de Seguridad y Privacidad de la Información que establece "*Elaborar una declaración de aplicabilidad que contenga: los controles necesarios, su estado de implementación y la justificación de posible exclusión*", y **el numeral 7.3.3. Plan de Tratamiento de los riesgos de seguridad de la información – Salidas (página 31) del documento maestro del Modelo de Seguridad y Privacidad de la Información** que establece "*Declaración de aplicabilidad, aceptada y aprobadas en el comité de gestión institucional*".

6.2.6. No se puede establecer o no se disponen los recursos que permitan la adopción, implementación, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información, ya que no se aportaron evidencias de la inclusión en los proyectos de inversión aquellas actividades relacionadas con la adopción del MSPI de acuerdo con el alcance establecido, incumpliendo el numeral **el numeral 7.4.1. Recursos - Lineamiento (página 32) del documento maestro del Modelo de Seguridad y Privacidad de la Información** que establece "*La entidad debe determinar y proporcionar los recursos necesarios para adoptar el MSPI, teniendo en cuenta que es un proceso transversal de la entidad, se requiere que se disponga de los recursos financieros, humanos (dedicación de horas/hombre) de sus colaboradores y en general cualquier recurso que permita la adopción, implementación, mantenimiento y mejora continua del MSPI*", y **el numeral 7.4.1. Recursos – Salidas (página 32) del documento maestro del Modelo de Seguridad y Privacidad de la Información** que establece "*Incluir dentro de los proyectos de inversión de la entidad aquellas actividades relacionadas con la adopción de MSPI de acuerdo con el alcance establecido*".

6.2.7. No se cuenta con un plan de capacitación de Seguridad y Privacidad de la Información para las vigencias 2022 y 2023 en el que se involucre al 100% de los servidores públicos de la entidad y asegure que estos cuenten con los conocimientos, educación y formación en seguridad y privacidad de la información para que se pueda realizar una adecuada implementación y gestión del modelo de seguridad y privacidad de la información. Tampoco se incluyeron capacitaciones relacionadas con seguridad y privacidad de la información en el PIC 2022 y 2023 conforme evaluación de estos en el sitio web de la entidad. Lo anterior, incumple el numeral 7.4.2. Competencia, toma de conciencia y comunicación - Lineamiento (página 33) del documento maestro del Modelo de Seguridad y Privacidad de la Información que establece "La entidad debe definir un plan de comunicación, capacitación, sensibilización y concientización para: … * Asegurar que las personas cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del modelo de seguridad y privacidad de la información. * Involucrar al 100% de los funcionarios de la entidad en la implementación y gestión del MSPI.", y el numeral 7.4.2. Competencia, toma de conciencia y comunicación - Salidas (página 33) del documento maestro del Modelo de Seguridad y Privacidad de la Información que establece "Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital. Este se puede incluir en el Plan Institucional de Capacitaciones - PIC".

6.2.8. No se puede establecer o no se dispone de un plan de implementación de controles de seguridad y privacidad de la información, ya que no fue aportado al ejercicio auditor, incumpliendo **el numeral 8.1. Planificación e implementación - Lineamiento (página 35) del documento maestro del Modelo de Seguridad y Privacidad de la Información** que establece "*La entidad debe realizar la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos, esta información debe estar documentada por proceso según lo planificado. Estos documentos deben ser aprobados por el comité institucional de gestión y desempeño*", y **el numeral 8.1. Planificación e implementación - Salidas (página 35) del documento maestro del Modelo de Seguridad y Privacidad de la Información** que establece "*Plan de implementación de controles de seguridad y privacidad de la información que contenga como mínimo: controles, actividades, fechas, responsable de implementación y presupuesto*".

7. SEGUIMIENTO AL PLAN DE MEJORAMIENTO DE AUDITORIAS ANTERIORES

Producto de auditoría realizada al proceso Gestión TICs en la vigencia 2021 se evidencia una (1) oportunidad de mejora y un (1) hallazgo relacionados con el Modelo de Seguridad y Privacidad de la Información, las cuales fueron cerradas en el seguimiento a los planes de mejoramiento realizados en marzo de 2022. Actualmente no hay oportunidades de mejora ni hallazgos relacionados con el Modelo de Seguridad y Privacidad de la Información abiertos.

8. SEGUIMIENTO AL MAPA DE RIESGOS DEL PROCESO.

El archivo aportado para el ejercicio auditor 08_1_Matriz de Riesgos UPME - Oficina_Gestión_Información_2023.xlsx da cuenta de los riesgos identificados por la Oficina de Gestión de Información y, teniendo en cuenta que no se suministraron más archivos, no es posible establecer si la entidad cuenta con la respetiva matriz de riesgos de seguridad y privacidad de la información para cada uno de los procesos de la Unidad de Planeación Minero Energética - UPME, conforme el modelo de operación por procesos de la Unidad.

Por otra parte, en el mes de noviembre se realizó seguimiento a los planes de mejoramiento existentes en la entidad, entre los que se encuentran los planes de mejoramiento suscritos por riesgos de gestión y corrupción, pero no se contemplaron los planes de mejoramiento suscritos por riesgos de seguridad y privacidad de la información, porque estos no se encuentran en el Sistema de Gestión Único Estratégico de Mejoramiento – SIGUEME.

9. RECOMENDACIONES

- Teniendo en cuenta que la implementación del Modelo de Seguridad y Privacidad de la Información es de vital importancia para la entidad, se recomienda la vinculación de toda su documentación al Sistema de Gestión Único Estratégico de Mejoramiento - SIGUEME.

- Realizar toda la gestión y administración de los riesgos de Seguridad y Privacidad de la Información en el Sistema de Gestión Único Estratégico de Mejoramiento – SIGUEME, tal como se hace con los riesgos de gestión y corrupción.

- Plan de Tratamiento de Riesgos contemple los lineamientos que el Modelo de Seguridad y Privacidad de la Información establece, tales como: Disponer de los controles pertinentes y apropiados para el tratamiento de riesgos, definir un plan que contenga fechas y responsables, definir la declaración de aplicabilidad que contenga los controles, su estado de implementación y la justificación de posible exclusión.

10. CONCLUSIÓN

La implementación de Modelo de Seguridad y Privacidad de la Información no ha contado con la participación activa de los Comités Institucionales de Gestión y Desempeño y Coordinación de Control Interno, generando que su implementación carezca de muchos de los instrumentos conforme lo establece el Modelo de Seguridad y Privacidad de la Información. De igual manera se detectan debilidades generales en la documentación requerida e instrumentos requeridos por este modelo para una adecuada gestión de la seguridad y privacidad de la información al interior de la Unidad de Planeación Minero Energética – UPME.

Así las cosas, se puede establecer que el grado de madurez promedio de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) conforme el documento del modelo versión 4 actualizado el 28 de octubre de 2021 es bajo, presentando un total de seis (06) oportunidades de mejora, ocho (08) hallazgos y tres (03) recomendaciones, así como las debilidades mencionadas en el presente informe.

LEONEL MAURICIO VELANDIA GÓMEZ
Profesional Especializado – Control Interno

INGRID CECILIA ESPINOSA SÁNCHEZ
Asesora de Control Interno (e)

Elaboró: Leonel Mauricio Velandia Gómez, Profesional Especializado Control Interno