INFORME DE AUDITORÍA

DEFINITIVO

Auditoría de Accesibilidad Web (NTC 5854) y Seguridad de la Información (MSPI)

OFICINA DE CONTROL INTERNO

YANETH RODRIGUEZ BUSTOS
JEFE DE LA OFICINA DE CONTROL INTERNO (E)

EQUIPO AUDITOR
RIGOBERTO ANDRES VACA PARDO

PERIODO EVALUADO
(VIGENCIA 2024 Y 2025)

FECHA DEL INFORME
(Octubre de 2025)
OCI-INFORME- 2025 -095

Contenido

1. INFORMACIÓN GENERAL 3
1.1. DESTINATARIOS DE LA AUDITORÍA 3
1.2. EQUIPO AUDITOR 3
2. OBJETIVO DE LA AUDITORÍA 3
3. ALCANCE DE LA AUDITORÍA 3
4. CRITERIOS 3
7. RESUMEN EJECUTIVO DE LOS RESULTADOS DE LA AUDITORIA 5
8. RESULTADOS DETALLADOS DE LA AUDITORIA 7
8.1. COMPONENTE AMBIENTE DE CONTROL 7
8.2 COMPONENTE EVALUACIÓN DEL RIESGO 10
8.3 COMPONENTE ACTIVIDADES DE CONTROL 15
8.4 COMPONENTE INFORMACIÓN Y COMUNICACIÓN 23
8.5 COMPONENTE ACTIVIDADES DE MONITOREO 38

1. INFORMACIÓN GENERAL

1.1. DESTINATARIOS DE LA AUDITORÍA

La presente auditoria tiene como destinatarios principales:

Secretario General
Coordinador de Grupo de Gestión de Tecnología
Oficina de Planeación y Gestión Internacional – Grupo de Gestión y Desempeño.
Coordinadora del Grupo de Comunicaciones y Prensa

1.2. EQUIPO AUDITOR

El equipo auditor asignado para llevar a cabo la presente evaluación es el siguiente:

Yaneth Rodríguez Bustos - Jefe de Oficina de Control Interno (E)
Rigoberto Andrés Vaca Pardo - Contratista.

2. OBJETIVO DE LA AUDITORÍA

Revisar y evaluar la eficacia la gestión de riesgo, control y gobierno del proceso Gestión de Tecnología de la Información y las Comunicaciones del Ministerio de Minas y Energía y los recursos del proyecto de inversión asociado al Fortalecimiento de las Capacidades tecnológicas.

3. ALCANCE DE LA AUDITORÍA

Realizar auditoría integral a la gestión del proceso de Gestión de Tecnología de la Información y las Comunicaciones, así como la evaluación de los controles, procedimientos e instructivos respectivos, correspondientes al período comprendido entre la vigencia 2024 y lo corrido de la vigencia 2025.

Nota: El establecimiento de este período no limita la facultad de la Oficina de Control Interno para pronunciarse sobre hechos previos o posteriores que, por su nivel de riesgo o materialidad, deban ser revelados

Limitaciones al Alcance: *Se describen en caso de existir*

4. CRITERIOS

- *Decreto Único Reglamentario del sector TIC 1078 de 2015*
- *Ley 1474 de 2011*
- *Ley 80 de 1993*
- *Ley 1712 de 2014*
- *Resolución 1519 de 2020 y sus anexos.*
- *Resolución 500 de 2021.*
- *Resolución 02277 de 2025.*

- *Documento Maestro del MSPI.*
- *Resolución 1978 de 2023.*
- *Decreto 612 de 2018*
- *Manual operativo de MIPG versión 6.*
- *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas versión 6 y 7.*
- *Políticas y Procedimientos internos de la Entidad.*

6. METODOLOGÍA

El presente ejercicio auditor se realizó en el marco de las Normas Internacionales de Auditoría Interna emitidas por el Instituto de Auditores Internos, el *"Estatuto de Auditoría de la Oficina de Control Interno del Ministerio de Minas y Energía"* y el *"Código de Ética de la Oficina de Control Interno del Ministerio de Minas y Energía"* aprobados por el Comité Institucional de Coordinación de Control Interno, así como los lineamientos establecidos para el Proceso Auditoria y Evaluación.

Planeación y desarrollo de la Auditoría:

Esta auditoría fue realizada con base en el análisis de diferentes muestras aleatorias seleccionadas por la auditora a cargo de la realización del trabajo. Una consecuencia de esto es la presencia del riesgo de muestreo, es decir, el riesgo de que la conclusión basada en la muestra analizada no coincida con la conclusión a que se habría llegado en caso de haber examinado todos los elementos que componen la población.

Como última etapa, con la información identificada y consolidada a lo largo del presente trabajo se construye el informe cuyos resultados se clasifican en conclusiones, observaciones y recomendaciones; cuyas definiciones se detallan a continuación:

- **Conclusiones**: Es el resumen de los aspectos principales analizados en el ejercicio auditor, los cuales están soportados en evidencias y pruebas realizadas.

- **Hallazgo:** Es el resultado de la comparación de La Condición (situación detectada o hechos identificados) con El Criterio que se refiere al deber ser (cumplimiento de normas, reglamentos, lineamientos o procedimientos). El hallazgo deben ser objeto de formulación de acciones tendientes a eliminar de fondo las causas que las originaron, las cuales harán parte del correspondiente plan de mejoramiento.

- **Oportunidad de mejora:** Situación que podría convertirse en un futuro incumplimiento de un requisito (observación) o materialización de un riesgo que podría llegar a tener efectos sobre el cumplimiento de los objetivos, procesos, planes, programas o proyectos. En caso de que, producto de análisis realizado, el proceso determine que se acogerán las oportunidades de mejora y se tomen medidas para su tratamiento o en caso de que sea requerido, las mismas deberán documentarse en el correspondiente plan de mejoramiento si la dependencia auditada así lo considera.

- **Recomendación:** Es una sugerencia encaminada a dar pautas para subsanar las causas identificadas en el ejercicio de auditoría realizado.

Es de aclarar que el término "**Plan de Mejoramiento**" hace referencia al instrumento que recoge y articula todas las acciones prioritarias que se emprenderán para mejorar aquellas características que tendrán mayor impacto en los resultados esperados, el logro de los objetivos de la entidad y la ejecución del plan de acción institucional. Su objetivo primordial es promover que la gestión de la entidad se desarrolle en forma eficiente y transparente, a través de la adopción y cumplimiento de las acciones correctivas y/o de la implementación de metodologías orientadas al mejoramiento continuo.

7. RESUMEN EJECUTIVO DE LOS RESULTADOS DE LA AUDITORIA

Tipo de Resultado	Consecutivo	Título	Proceso / Área Responsable	Plan de Mejoramiento	Componente de Control Interno que afecta	Dimensión MIPG que afecta
Hallazgo	H-01-2025	Incumplimiento en la Identificación de Requisitos de las Partes Interesadas	Grupo de Trabajo de tecnología de la Información	Obligatorio	Ambiente de Control	Direccionamiento Estratégico y Planeación
Hallazgo	H-02-2025	Debilidades en la planificación y tratamiento de riesgos	Grupo de Trabajo de tecnología de la Información	Obligatorio	Evaluación del Riesgo	Gestión con Valores para Resultados Control Interno
Hallazgo	H-03-2025	Debilidad en la aplicación de controles de desarrollo seguro.	Grupo de Trabajo de tecnología de la Información	Obligatorio	Actividades de Control	Gestión con Valores para Resultados
Hallazgo	H-04-2025	Incumplimiento de condiciones de Accesibilidad en página web.	Grupo de Comunicaciones y Prensa.	Obligatorio	Actividades de Control Información y Comunicación	Gestión con Valores para Resultados Información y Comunicación
Hallazgo	H-05-2025	Debilidades en la aplicación del estándar de publicación de información mínima.	Grupo de Comunicaciones y Prensa.	Obligatorio	Actividades de Control Información y Comunicación	Gestión con Valores para Resultados Información y Comunicación
Hallazgo	H-06-2025	Información de la Entidad sin fecha de publicación en la página web	Grupo de Comunicaciones y Prensa.	Obligatorio	Actividades de Control Información y Comunicación	Gestión con Valores para Resultados Información y Comunicación

Tipo de Resultado	Consecutivo	Título	Proceso / Área Responsable	Plan de Mejoramiento	Componente de Control Interno que afecta	Dimensión MIPG que afecta
Hallazgo	H-07-2025	Incumplimiento en la medición del Desempeño del Sistema de Gestión de Seguridad de la Información	Grupo de Trabajo de tecnología de la Información. Oficina de Planeación y Gestión Internacional	Obligatorio	Actividades de Control Actividades de Monitoreo	Gestión con Valores para Resultados Evaluación de Resultados
Hallazgo	H-08-2025	Debilidades en la revisión por la Dirección	Grupo de Trabajo de tecnología de la Información. Oficina de Planeación y Gestión Internacional	Obligatorio	Actividades de Control Actividades de Monitoreo	Gestión con Valores para Resultados Evaluación de Resultados
Hallazgo	H-09-2025	Debilidades en la implementación de acciones de mejora	Grupo de Trabajo de tecnología de la Información	Obligatorio	Actividades de Control Actividades de Monitoreo	Gestión con Valores para Resultados Evaluación de Resultados
Oportunidad de Mejoramiento	OM-01-2025	Planificación y ejecución de pruebas de backup	Grupo de Trabajo de tecnología de la Información Y Grupo de Comunicación y Prensa	Voluntario	Actividades de Control	Gestión con Valores para Resultados Información y Comunicación
Oportunidad de Mejoramiento	OM-02-2025	Publicación de Documentación del Proceso	Grupo de Trabajo de tecnología de la Información Y Oficina de Planeación y Gestión Internacional – Grupo de Gestión de Desempeño	Voluntario	Información y Comunicación	Información y Comunicación

8. RESULTADOS DETALLADOS DE LA AUDITORIA

8.1. COMPONENTE AMBIENTE DE CONTROL

La verificación del presente componente se llevó a cabo teniendo en cuenta los lineamientos y directrices emitidos por el Ministerio de Minas y Energía, con la finalidad de identificar su eficiencia y aplicación, en lo relacionado con la gestión de Tecnologías de Información y las Comunicaciones de la Entidad y su adherencia con los lineamientos emitidos por MinTIC para la Gestión de Seguridad de la Información en el marco de implementación del Modelo de Seguridad y Privacidad de la Información – MSPI.

Compromiso de la línea Estratégica

Se evidenció que la Entidad ha dispuesto distintos recursos, mecanismos, políticas, entre otras, para disponer de un ambiente de control en materia de gestión de tecnología de información y comunicaciones las cuales se relacionan con:

1. Definición de Políticas, Roles y Responsabilidades de Seguridad de la Información

- El Ministerio de Minas y Energía ha formalizado las políticas de seguridad de la Información, a través de la resolución 40646 del 11 de noviembre de 2023.
- A través de los artículos 7, 8, 9 y 10 de la resolución 40646 se establecen los roles y responsabilidades del Comité Institucional de Gestión y Desempeño, así como la definición del rol del Oficial de seguridad de la Información y sus responsabilidades.

2. Destinación de recursos para:

- "*Fortalecimiento de las Capacidades tecnológicas del Ministerio de Minas y energía para facilitar el uso, acceso y aprovechamiento de la información minero-energética a Nivel Nacional*" a través del proyecto identificado con código BPIN 2020011000126.
- "*Fortalecimiento de la capacidad del Ministerio de Minas y Energía para implementar de manera efectiva la política de gobierno digital Nacional*" a través del proyecto identificado con código BPIN 202400000000198.

3. Asignación de Talento Humano y definición políticas para la gestión de Tecnologías de la Información y las Comunicaciones evidenciadas en los siguientes documentos:

- Asignación de funciones a fin de *"Proponer la adopción de políticas para el buen manejo y seguridad de la información sistematizada en el Ministerio, y promover el desarrollo e implementación de programas sistematizados"* a la Secretaría General mediante Decreto 030 de 2022.
- Definición de Grupo de trabajo y designación del Oficial de seguridad de la Información.
- Adopción de las políticas aplicables al Talento Humano en concordancia con el Modelo de Seguridad y Privacidad de la Información — MSPI del Ministerio de Minas y Energía, mediante resolución 40646 del primero de noviembre de 2023.
- Definición del rol de Oficial de Seguridad.

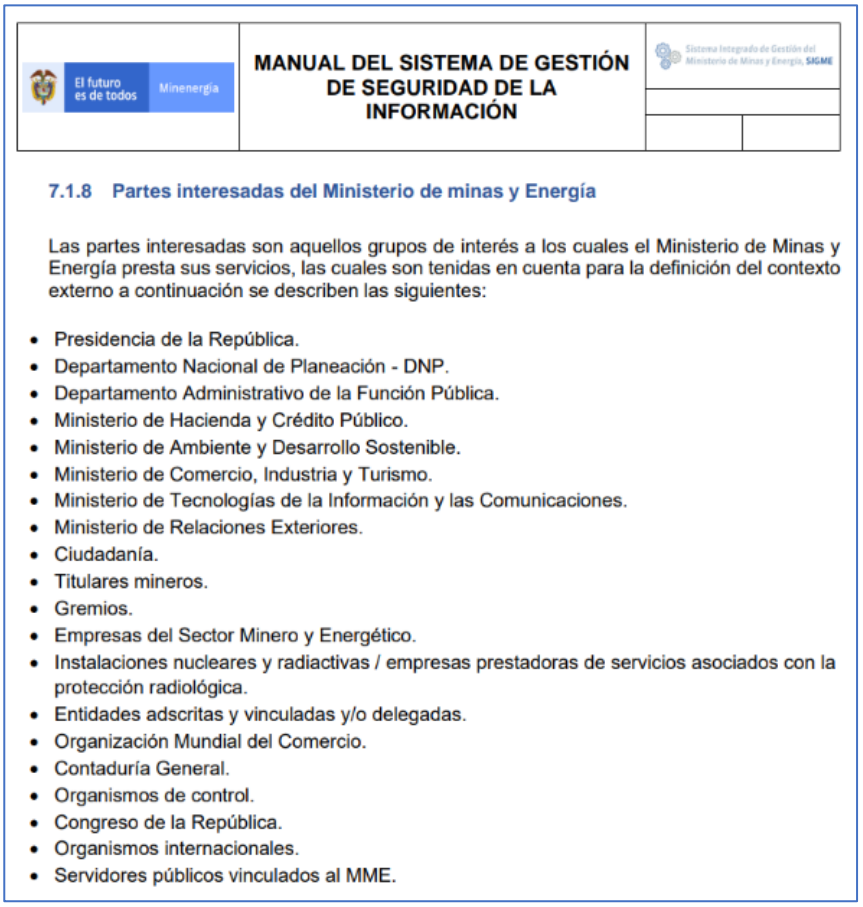
4. Articulación con la Planeación Institucional:

- Se observa que los planes (i)Plan estratégico de Tecnologías de la Información – PETI, (ii) Plan de tratamiento de riesgos de seguridad de la información y (iii) Plan de seguridad y privacidad de la información, fueron aprobados por el Comité Institucional de Gestión y Desempeño en concordancia con los lineamientos del decreto 612 de 2018.

HALLAZGO N° 01 – Incumplimiento en la Identificación de Requisitos de las Partes Interesadas

Condición:

Se identificó en el desarrollo de la auditoría, que, como parte del ejercicio de planeación y estructuración del sistema, se han identificado las partes interesadas dentro del Manual del Sistema de Gestión de Seguridad de la Información aportado por el área auditada en el desarrollo de la auditoría, según se muestra en la imagen a continuación:



El futuro es de todos | Minenergía

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Sistema Integrado de Gestión del Ministerio de Minas y Energía, SIGME

7.1.8 Partes interesadas del Ministerio de minas y Energía

Las partes interesadas son aquellos grupos de interés a los cuales el Ministerio de Minas y Energía presta sus servicios, las cuales son tenidas en cuenta para la definición del contexto externo a continuación se describen las siguientes:

- Presidencia de la República.
- Departamento Nacional de Planeación - DNP.
- Departamento Administrativo de la Función Pública.
- Ministerio de Hacienda y Crédito Público.
- Ministerio de Ambiente y Desarrollo Sostenible.
- Ministerio de Comercio, Industria y Turismo.
- Ministerio de Tecnologías de la Información y las Comunicaciones.
- Ministerio de Relaciones Exteriores.
- Ciudadanía.
- Titulares mineros.
- Gremios.
- Empresas del Sector Minero y Energético.
- Instalaciones nucleares y radiactivas / empresas prestadoras de servicios asociados con la protección radiológica.
- Entidades adscritas y vinculadas y/o delegadas.
- Organización Mundial del Comercio.
- Contaduría General.
- Organismos de control.
- Congreso de la República.
- Organismos internacionales.
- Servidores públicos vinculados al MME.

Fuente: Manual del SGSI aportado por el Grupo TIC's

No obstante, lo anterior, no se evidenció la documentación y/o registro del compendio de necesidades y expectativas de las partes interesadas relacionadas con la seguridad de la información, en concordancia con los documentos obligatorios requeridos en el numeral 7.1.2. Necesidades y expectativas de los interesados del MSPI.

Criterio(s):

Resolución 02277 de 2025 *""Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia"*

"ARTÍCULO 1*. Actualización del Anexo 1 de la Resolución 500 de 2021. Actualícese el Anexo 1 de la Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", el cual será publicado en la sede electrónica del Ministerio de Tecnologías de la Información y las Comunicaciones, a más tardar quince (15) días siguientes a la expedición de la presente resolución".*

Anexo 1 de la Resolución 02277 - Modelo de Seguridad y Privacidad de la Información:

7.1.2. Necesidades y expectativas de los interesados del Modelo de seguridad y Privacidad de la Información

"Se deben identificar las partes interesadas internas y externas que puedan influir o verse afectadas por la seguridad y privacidad de la información, así como sus necesidades y expectativas."

Norma ISO 27001 numeral 4.2

"*4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS*
La organización debe determinar:

a) las partes interesadas que son pertinentes al sistema de gestión de la seguridad de la información; y
b) los requisitos de estas partes interesadas pertinentes a seguridad de la información."

Manual operativo de MIPG versión 6

Dimensión 2: Direccionamiento Estratégico y Planeación

2.2 Política de Planeación institucional

Lineamientos generales para la implementación de la política:

"(...) ¿Para quién y para qué lo debe hacer?: Es necesario caracterizar, a qué grupo de ciudadanos debe dirigir sus productos y servicios (grupos de valor) y para qué lo debe hacer, es decir, cuáles son los derechos que se deben garantizar, qué necesidades se deben satisfacer, qué problemas se deben solucionar y qué información que debe suministrar.(...)"

Posible(s) causa(s) identificada(s) por la Oficina de Control Interno

- Debilidades en la adopción de elementos de planificación y documentos obligatorios del MSPI.
- Falta de conocimiento en la implementación de los requisitos del Modelo de Seguridad y Privacidad de la Información.
- Debilidad en el seguimiento y actualización de necesidades y expectativas de los grupos de valor y partes interesadas del Ministerio de minas y Energía

Posible(s) Consecuencias o efectos (s) identificado(s) por la Oficina de Control Interno

- Inadecuado tratamiento de riesgos oportunidades de seguridad de la información.
- Posible afectación a la toma de decisiones estratégicas en materia de seguridad de la información por desconocimiento del comportamiento de los indicadores.
- Posible debilidad en la implementación de controles al no contar con elementos requeridos para la planeación y estructuración del Sistema de Gestión de Seguridad de la Información.
- Posible desactualización del Manual del Sistema de Gestión de Seguridad de la Información que data de la vigencia 2021.

Recomendación(nes) específica(s):

- Aplicar evaluaciones del modelo de madurez en la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI así como del Modelo de Referencia de Arquitectura Empresarial en lo relacionado con la implementación del MSPI.
- Adelantar los tramites internos de actualización y formalización de manuales y procedimientos dentro del SIG, de manera articulada con la OPGI.

8.2 COMPONENTE EVALUACIÓN DEL RIESGO

Para este componente se llevó a cabo la verificación de los lineamientos de implementación de la gestión y tratamiento de riesgos por parte de la segunda línea de defensa, acorde a las directrices dadas por el Documento Maestro del MSPI en concordancia con lo establecido en la resolución 02277 de 2025 y resolución 500 de 2021.

En este sentido se identificó en primera instancia que la Entidad ha definido directrices para la evaluación y gestión de riesgos a través del manual de gestión de riesgos y oportunidades identificado con código E-ME-M-02, sin embargo, es preciso mencionar que a partir de los resultados de la auditoría interna adelantada por la Oficina de Control Interno al proceso de Gestión de Tecnologías de la Información y las Comunicaciones, durante la vigencia 2025, se identificaron debilidades en la actualización de activos de información y la consecuente identificación de amenazas y vulnerabilidades asociadas inherentes a los activos, las cuales deben ser identificadas acorde a los lineamientos del Modelo Nacional de Riesgos de Seguridad Digital.

En este sentido es pertinente mencionar que la Entidad se encuentra en proceso de actualización de la matriz de activos de información como punto de partida para la identificación evaluación y tratamiento de riesgos de seguridad de la información.

Dado lo anterior, con el objetivo de subsanar las causas asociadas al hallazgo y atendiendo los lineamientos internos de la Entidad, se formuló el plan de mejoramiento identificado con código PM-25-AI2025-20, el cual se encuentra en curso de implementación.

De otra parte, es importante mencionar que según lo confirmado por el área auditada en sesión del pasado 8 de septiembre, a partir de los resultados obtenidos en la evaluación FURAG, se definió como parte de las acciones de mejoramiento, la actualización del manual de gestión de riesgos y oportunidades a fin de fortalecer entre otros aspectos, los lineamientos metodológicos para la gestión de riesgos de seguridad de la información, así como la identificación de amenazas y vulnerabilidades.

En este sentido se observan debilidades en la identificación valoración y clasificación de activos como punto de partida para la identificación y evaluación de riesgos de seguridad de la información, las cuales están siendo tratadas por las áreas involucradas a través de los planes de mejoramiento en curso.

De otra parte, se evidenció que la Entidad definió (i) el Plan de tratamiento de riesgos de seguridad de la información y (ii) Plan de seguridad y privacidad de la información, y que los mencionados documentos fueron aprobados por el Comité Institucional de Gestión y Desempeño en concordancia con los lineamientos del decreto 612 de 2018.

También se observó que se realizan y publican informes de seguimiento de manera trimestral según se evidencia en la siguiente imagen tomada de la sección de transparencia de la Entidad.

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información:

- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025
- Seguimiento Primer Trimestre - Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025
- Seguimiento Segundo Trimestre - Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025

Plan de Seguridad y Privacidad de la Información:

- Plan de Seguridad y Privacidad de la Información 2025
- Seguimiento Primer Trimestre - Plan de Seguridad y Privacidad de la Información 2025
- Seguimiento Segundo Trimestre - Plan de Seguridad y Privacidad de la Información 2025

Fuente: página web de la Entidad

HALLAZGO Nº 2 - Debilidades en la planificación y tratamiento de riesgos

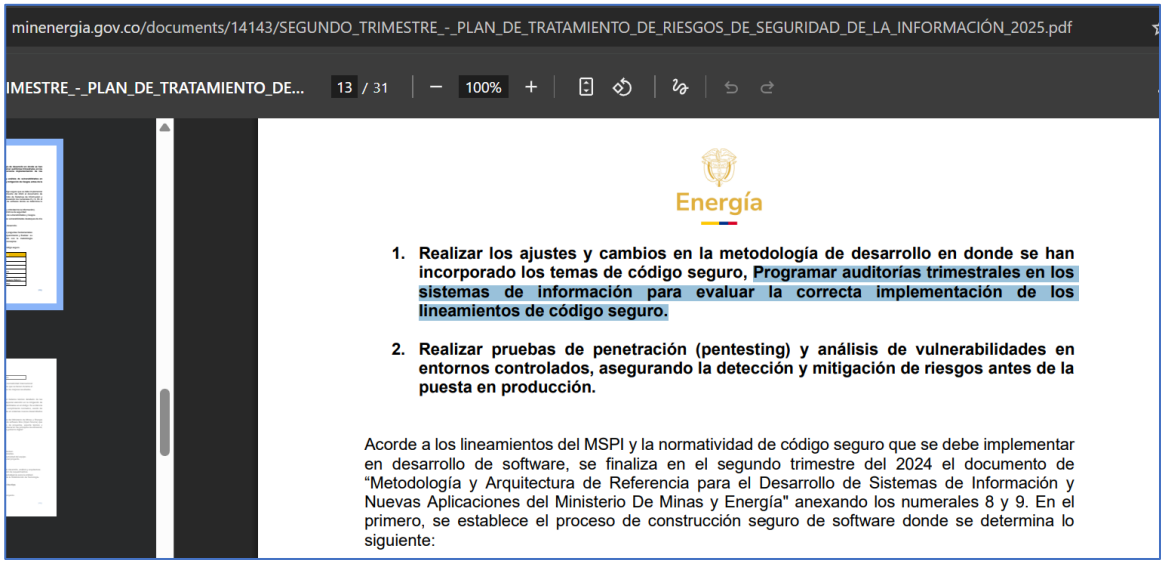
Condición:

La Oficina de Control Interno, a parir de los lineamientos dados por el Documento Maestro del MSPI, el cual, en su numeral 7.3.3. Plan de tratamiento de los riesgos de seguridad de la información establece las directrices para el tratamiento de riesgos, evaluó el estado de implementación de los controles del Sistema de Gestión de Seguridad de la Información evidenciando lo siguiente:

1. Acorde a la información entregada por el Grupo de Tecnología de la Información y las Comunicaciones, se aportó el archivo de Excel "Matriz_de_Evaluacion,_Aplicabilidad_SOA MINENERGIA", en el que se describe el estado de implementación por parte de la Entidad para los controles requeridos por MSPI.
2. A partir del estado de implementación que se relaciona en el archivo anteriormente referenciado, se identificó un nivel de implementación del 37,35% correspondiente a 31 controles que se indican como implementados.

Estado del Control	Cantidad de Controles
En implementación	48
Implementado	31
Necesario/No implementado	4
Total general	**83**

   En consecuencia, se identifica por parte del Grupo de Tecnología que falta por terminar la implementación del 62,65% de los controles; en donde se identifica adicionalmente que un 57,83% de los controles se encuentran en proceso de implementación (48 controles) y un 4,82% se identifican como Necesario/No Implementado, lo cual denota un nivel incipiente/inicial de implementación de los controles requeridos por la Norma ISO 27001 y el MSPI.
3. Acorde a lo confirmado por el Grupo de Tecnología de Información y las Comunicaciones, en sesión de auditoría del 8 de septiembre de 2025, la declaración de aplicabilidad no se encuentra aprobada por el Comité Institucional de Gestión y Desempeño.
4. Según lo evidenciado en el segundo informe de seguimiento al plan de tratamiento de riesgos publicado en la página web de la Entidad, se definió como actividad de tratamiento "(...) *Programar auditorías trimestrales en los sistemas de información para evaluar la correcta implementación de los lineamientos de código seguro*. (...)", según se observa en la siguiente imagen:



No obstante, al requerir los soportes de ejecución de la actividad, se informó por parte del área auditada en sesión del pasado 8 de septiembre que no se tienen programación y no se está cumpliendo con esta actividad, de otra parte, también se confirmó en la sesión que no se presentan observaciones respecto a la desviación en la aplicación del control y/o actividad de tratamiento.

Teniendo en cuenta lo anteriormente mencionado se evidencia incumplimiento de los lineamientos dados por el MSPI para el tratamiento de riesgos de seguridad de la Información toda vez, que (i) no se ha aceptado la declaración de aplicabilidad por parte del Comité Institucional de Gestión y Desempeño, (ii) se evidenció la falta de aplicación de actividad de tratamiento de riesgos de seguridad de la información relacionados con la evaluación de los sistemas de información y el cumplimiento de lineamientos de código seguro.

Criterio(s):

Resolución 02277 de 2021 *"Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia"*

"ARTÍCULO 1*. Actualización del Anexo 1 de la Resolución 500 de 2021. Actualícese el Anexo 1 de la Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", el cual será publicado en la sede electrónica del Ministerio de Tecnologías de la Información y las Comunicaciones, a más tardar quince (15) días siguientes a la expedición de la presente resolución".*

Anexo 1 de la Resolución 02277 - Modelo de Seguridad y Privacidad de la Información:

7.3.3. Plan de tratamiento de los riesgos de seguridad de la información

(...) Las entidades deben definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información, que permita:
• Seleccionar las opciones (controles) pertinentes y apropiadas para el tratamiento de riesgos.
• Elaborar una declaración de aplicabilidad que contenga: los controles adoptados por la entidad, su estado de implementación y la justificación de posible exclusión de acuerdo con los riesgos identificados y las capacidades técnicas y humanas con las que cuenta.
• Definir un plan de tratamiento de riesgos que contenga, fechas, acciones de tratamientos de riesgos a tratar y responsables con el objetivo de realizar trazabilidad. (...)

*"**Salidas**: (...) Declaración de aplicabilidad, aceptada y aprobadas en el comité institucional de gestión y desempeño (...)".*

8.2. Plan de tratamiento de riesgos

"(...) La entidad debe conservar información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información.
• La entidad debe implementar el plan de tratamiento de riesgos de seguridad de la información (...)".

Modelo Integrado de Planeación y Gestión (MIPG) Dimensión 4: Evaluación de Resultados

*"**Lineamientos generales para la implementación***

(...) Evaluar el logro de los resultados
Para ello, se debe aplicar los indicadores definidos de acuerdo con las decisiones que la entidad haya asumido y las disposiciones establecidas en las normas y lineamientos de política frente a las maneras, plazos y poblaciones a quienes decide entregar la información del seguimiento y evaluación (...)

Posible(s) causa(s) identificada(s) por la Oficina de Control Interno

- Debilidades en la adopción de herramientas de medición del desempeño de seguridad.
- Falta de adopción de buenas prácticas de gestión de seguridad de la información.
- Debilidad en la apropiación de conocimientos y habilidades para la medición del desempeño de seguridad de la información.
- Debilidad en el seguimiento y control de indicadores de seguridad de la Información diseñados.

Posible(s) Consecuencias o efectos (s) identificado(s) por la Oficina de Control Interno

- Inadecuado tratamiento de riesgos oportunidades de seguridad de la información.
- Posible afectación a la toma de decisiones estratégicas en materia de seguridad de la información por desconocimiento del comportamiento de los indicadores.

Recomendación(nes) específica(s):

- Evaluar la pertinencia de aplicar evaluaciones del modelo de madurez en la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI así como del Modelo de Referencia de Arquitectura Empresarial y sus componentes.
- Adelantar los tramites internos de formalización de procedimientos aplicables a la gestión de riesgos, gestión de tecnología y gestión de seguridad de la información dentro del SIG, de manera articulada con la OPGI.

8.3 COMPONENTE ACTIVIDADES DE CONTROL

Con el objetivo de verificar las actividades de control, se adelantó revisión de la implementación de controles relacionados con la gestión de desarrollo de software, gestión de incidentes, entre otros establecidos por el Modelo de Seguridad y Privacidad de la Información.

Al respecto es importante mencionar que en el desarrollo de la auditoría adelantada por la Oficina de Control Interno durante la vigencia 2025, en la cual se evaluó la gestión del proceso de Tecnología de la Información y las Comunicaciones, se identificaron hallazgos relacionados con la aplicación de controles de seguridad física y la operación de la mesa de ayuda, a partir de los cuales se generaron los planes de mejoramiento identificados con los códigos: PM-25-AI2025-20 (riesgos de seguridad de la información), PM-25-AI2025-21 (Gestión de Riesgos), PM-25-AI2025-22 (Controles de Seguridad Física), PM-25-AI2025-22 (Mesa de Ayuda).

A partir de lo anterior se evaluaron controles relacionados con la ejecución de copias de respaldo, desarrollo seguro y gestión de incidentes.

En lo relacionado con la gestión de copias de respaldo (Backup), se identificó que la Entidad cuenta con la herramienta ArcServe a través de la cual se realiza la programación de las copias y se ejecutan de manera automática.

En el ejercicio de auditoría se evidenció que la herramienta ArcServe conserva el registro de las copias realizadas y en caso de presentarse algún error, la herramienta reintenta hasta poder realizar la copia de manera exitosa.

De otra parte, teniendo en cuenta que el control A.8.13 “Copias de seguridad de la información” establece:

"Las copias de seguridad (respaldos) de la información, del software y de los sistemas deben mantenerse y probarse periódicamente de conformidad con la política de copia de seguridad específica del tema acordado."

Se indagó respecto de la planificación y ejecución de pruebas de las copias de respaldo identificando que se realizan algunas pruebas específicas solicitadas por demanda; sin embargo, no se cuenta con la planificación periódica de realización de pruebas. **(Ver oportunidad de mejora No. 1)**

OPORTUNIDAD DE MEJORA Nº 1 – Planificación y ejecución de pruebas de backup

Como resultado de la revisión de la aplicación de controles de copias de respaldo se identificó que, aunque se han realizado algunas pruebas por demanda, no se cuenta con una planificación periódica de realización de pruebas, a fin de asegurar que las copias funcionen adecuadamente en el momento en que se requieran y que adicionalmente la información respaldada pueda ser recuperada acorde a los RTO (Recovery Time Objective) definidos.

Recomendación(nes) específica(s):

- Fortalecer la planificación de ejecución de pruebas de backup, a fin de asegurar que los sistemas de información, bases de datos, servidores, entre otros activos críticos cuenten con copias de respaldo probadas y completas.
- Evaluar el cumplimiento de los tiempos de recuperación de las copias de respaldo a fin de cumplir con los RTO (Recovery time Objective) definidos.

HALLAZGO Nº 3 – Debilidad en la aplicación de controles de desarrollo seguro.

Condición:

En sesión de auditoría del pasado 5 de septiembre se realizó prueba de verificación de cumplimiento de lineamientos de seguridad de la información para el desarrollo seguro en 3 aplicativos desarrollados (In house) identificados como (Buzón de integridad y transparencia, SIFGAME y Ventanilla) tomados como muestra y en concordancia con lo registrado en el archivo de excel "CATÁLOGO O DIRECTORIO DE SIS-INF old", aportado por el área auditada evidenciando lo siguiente:

1. **Frente a las pruebas de seguridad:**

   Se indicó por parte del área auditada que la metodología de desarrollo se encuentra en proceso de actualización, por lo que los lineamientos específicos en relación con la aplicación de pruebas se encuentran en el documento "Manual – Metodología y arquitectura de referencia para el desarrollo de sistemas de información y nuevas aplicaciones", según se muestra en la imagen a continuación:

En el documento se describen los siguientes tipos de pruebas de seguridad:

a) Pruebas Unitarias.
b) Pruebas de Integración.
c) Pruebas de Regresión.
d) Pruebas de Humo.
e) Pruebas de desempeño.
f) Pruebas de Carga.
g) Pruebas de Stress.
h) Pruebas de Volumen.
i) Pruebas de recuperación y tolerancia a Fallas.
j) Pruebas de Seguridad.
k) Entre otras.

En el cual, no se establecen lineamientos específicos para el desarrollo de pruebas de código estático, en este sentido se argumentó por parte del proceso que se encuentra relacionada la categoría "entre otras", la cual abarca otros tipos de pruebas, por lo que se indagó por las pruebas de código estático realizadas en los aplicativos tomados como muestra, (Buzón de integridad y transparencia, SIFGAME y Ventanilla Única de Trámites), para lo cuales se confirmó que no se han realizado pruebas de código estático.

De otra parte, según lo indicado por el equipo de desarrollo en sesión del pasado 10 de septiembre de 2025, "no se tiene un plan de pruebas para ejecutar las pruebas de seguridad", por parte del equipo de desarrollo.

*Por tanto, teniendo en consideración que (i) no se cuenta con una planificación de las pruebas de seguridad, y que (ii) la metodología de desarrollo aún no se encuentra aprobada, se evidencian debilidades en la aplicación de controles de pruebas de seguridad en el desarrollo de software (**Control A.8.29 del MSPI**), adicionalmente (iii) al no contemplar las pruebas de código estático y no contar evidencia de su realización se evidencia el incumplimiento del numeral **3.3 PROGRAMACIÓN DEL CÓDIGO FUENTE del Anexo 3 dela resolución 1519 de 2020.***

2. ***Frente a los controles de versionamiento de software.***

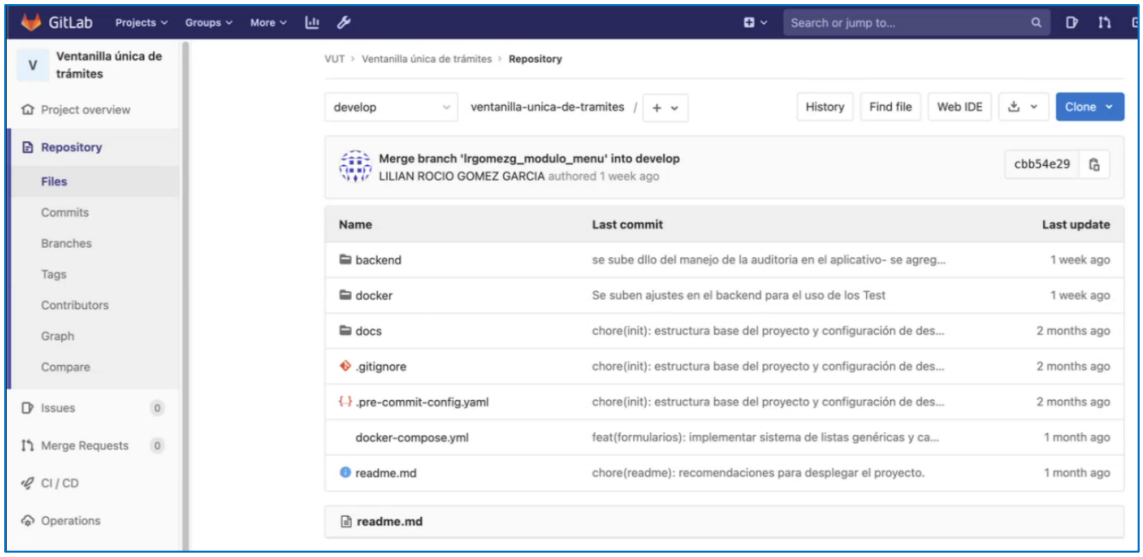
Se identificó en primera instancia que, dentro del catálogo de sistemas de información aportado por el área auditada, no se registra la versión de software en todos los casos, según se aprecia a continuación:

ID	NOMBRE	SIGLA	DESCRIPCIÓN	CATEGORÍA	PROCESO(S) QUE SOPORTA	FUNCIONALIDADES O MODULOS	ENTRADAS	SALIDAS	ESTADO	VERSIÓN
1	PROCESO DE PLANEACIÓN ESTRATÉGICA - SIGAME	SIGAME	Sistema de Información que permite definir indicadores de gestión mediante la definición de objetivos, planes de acción, metas e indicadores de desempeño.	Estratégicos	Direccionamiento Estratégico	Administración de usuarios. Administración general. Módulo de planeación estrategica (Procesos y procedimientos). Módulo de plan de accón(metas, indicadores, productos, seguimiento Módulo de riesgos. Módulo documental de los procesos SGG. Módulo normograma. Módulo de auditoria interna SGC. Módulo de plan de mejoras. Reportes y tableros de control. MÓDULO DE PROYECTOS ??	Planes estrategicos, procesos, procedimientos, planes de accion, planes de mejora, riesgos, los indicadores, normagrama, seguimientos.	Auditorias de procesos, reportes, tableros de control, informes de gestión con ponderación de avance.	En producción	N/A
5	SUBSIDIOS GLP EN CILINDROS	GLP	Permite el registro de subsidios al consumo de GLP en cilindros para los departamentos de Nariño, Putumayo, Caquetá, San Andrés y providencia y en las áreas rurales de cinco municipios del departamento del Cauca. Conformada por una aplicación web usada por las empresas, usuarios y el ministerio; y una aplicación móvil usada por los vendedores de las empresas	Misionales	Hidrocarburos	Administracion. Empresas. Operadores Vendedores.	Vendedores, empresas, cilindros, registroo de subsidios, beneficiarios	Reportes y consolidados de subsidios reistrados	En producción	N/A
6	SEGUIMIENTO A PROYECTOS FINANCIADOS A TRAVÉS DEL FONDO ESPECIAL CUOTA DE FOMENTO - SUNA	SUNA	Sistema para el seguimiento a proyectos de cofinanciación del fondo especial cuota de fomento. Es una aplicación web para el registro de los diferentes documentos y actividades realizadas por las empresas ejecutoras, la interventoria del fondo y el ministerio.	Misionales	Hidrocarburos	Operadores redes gas natural. Transportadores de red de gas natural(Gasoductos). Proyectos. Convenios. Financiero Administración.	Documentos e información de proyectos de confinanciación de redes de Gas Natural.	Reportes	En producción	N/A
7	SISTEMA DECLARACIÓN DE GAS	SDG	Sistema de información sirve para la captura, análisis y consolidación de la Declaración de Producción de Gas Natural aportada por los agentes Productores y Productores-Comercializadores. Se genera una proyecto a 10 años de la producción de gas. Cada año se debe generar esta proyección por los productores.	Misionales	Hidrocarburos	Modulo Administración. Módulo Operadores o Asociados	Decalraciones de producción en formato excel de cada campo contrato(Operador y Asociado, potencial de producción del campo).	Declaración nacional de produccion en formato excel.	En producción	N/A
8	SISEG COMPONENTE HIDROCARBUROS	SISEG HIDROCARBUROS	Sistema de Información para la administración del Fondo de Solidaridad para Subsidios y Redistribución de Ingresos de los servicios públicos domiciliarios de energía eléctrica y de gas combustible distribuido por red física y del Fondo de Energía Social FOES	Misionales	Hidrocarburos	Administración. Operadores de gas por redes.	Subsidios, contribuciones, giros y excentos en excel.	Informe consolidado de subsidios y contribuciones por operador	En producción	2.8.8
9	SISTEMAS DE INFORMACIÓN DE TRANSPORTE DE HIDROCARBUROS	SITH	Sistema de Información para el Transporte de Hidrocarburos diseñado para facilitar el registro y la actualización periódica de las tarifas del servicio de transporte, además de automatizar la generación trimestral de las liquidaciones correspondientes, discriminando entre municipios productores y no productores, conforme a la normativa vigente.	Misionales	Hidrocarburos	Administracion. Operadores. Tarifas transporte. Liquidación.	Documentos de excel con volumenes de GN transportados.	Reportes liquidación y preliquidacion del transporte hidrocarburos.	En producción	N/A
15	PORTAL WEB	SEDE ELECTRONCIA	Permite mantener informada a la entidad y a la ciudadanía en general respecto a su estructura organizacional, normatividad, conceptos del uso de la energía y recursos naturales; cumpliendo los lineamientos establecidos en Gobierno Digital	Transversales	Procesos Misionales y Estratégicos	Portal Digital CMS PQRSD INDY Chatbot	PQRSD	Respuesta PQRSD	En producción	
16	INTRANET	INTRANET	Permite mantener informada a los funcionarios y colaboradores de la entidad y a respecto a su estructura organizacional interna, normatividad, conceptos de uso y apropiación de la plataforma; cumpliendo los lineamientos establecidos por el Ministerio de Minas y Energía	Transversales	Procesos Transversales	Portal Digital CMS	Consultas información	Respuesta	En producción	
17	EITI COLOMBIA	EITI	Desarrollo web mediante el cual Colombia muestra su participación en la Iniciativa de Transparencia de las Industrias Extractivas (EITI), el cual es un Estándar mundial que promueve la gestión abierta y responsable de los recursos del petróleo, gas y minerales.	Estratégicos	Direccionamiento Estratégico	Portal Digital CMS	Consultas información	Respuesta	En producción	
18	BUZON DE INTEGRIDAD Y TRANSPARENCIA	LINEA ETICA	Descripción Linea ética: A través de esta plataforma, de manera confidencial y anónima si así se desea, funcionarios, contratistas, usuarios y ciudadanos pueden denunciar o informar posibles hechos de corrupción, conflictos de interés, cobro de trámites gratuitos, acoso laboral y sexual y todo tipo de conductas que se consideren irregulares e involucren a funcionarios y/o contratistas del Ministerio de Minas y Energía y las entidades adscritas y vinculadas del sector.	Estratégicos	Procesos Misionales y Estratégicos	Portal Digital CMS Denuncias Ciudadanas	Consultas información Denuncias	Respuesta	En producción	

De otra parte, se evidenció lo siguiente:

Para el software Ventanilla Única de Trámites,

Se indicó en primera instancia que este aplicativo se encuentra en proceso de desarrollo y por tanto no se encuentra implementado en ambiente de producción, sin embargo, se evidenció que se cuenta con un repositorio en el que se encuentra el código fuente, según se muestra a continuación:

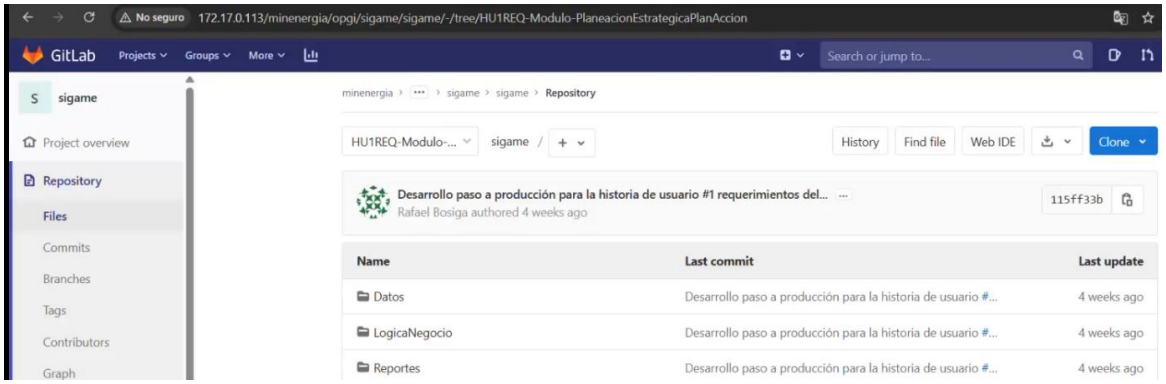


Al respecto, se indicó también que este software fue recibido y se tuvo que hacer *"reingeniería"* para continuar con su desarrollo.

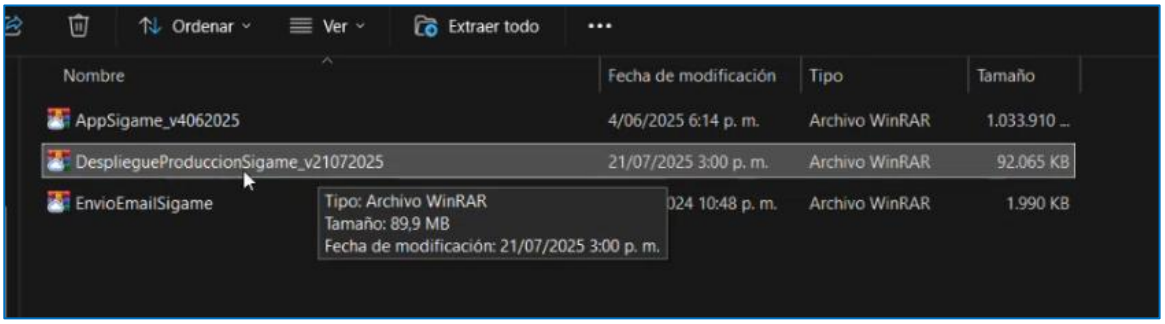
De acuerdo con lo anterior, no se observó que se haya definido el esquema de versionamiento o esquema de "ramas" para el proyecto, entendiendo que el control de versionamiento se aplica desde la etapa de desarrollo y según se informó por parte del personal técnico, la versión que se lanzará será la primera.

Para el software SIGAME

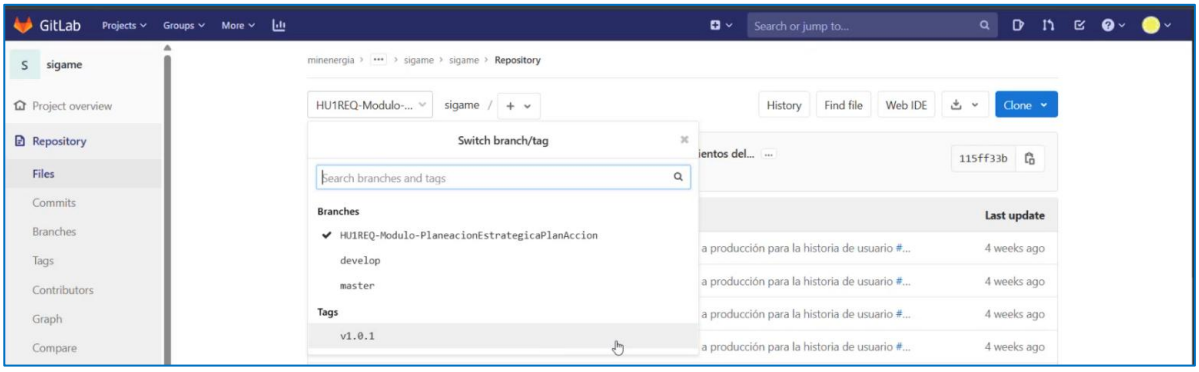
Se observó que se cuenta con repositorio en la herramienta GITLab, según se muestra a continuación:



Sin embargo, se indicó que el versionamiento del software se documentó en el archivo de despliegue (instalador), acorde a la fecha de publicación, según se muestra en la imagen a continuación:



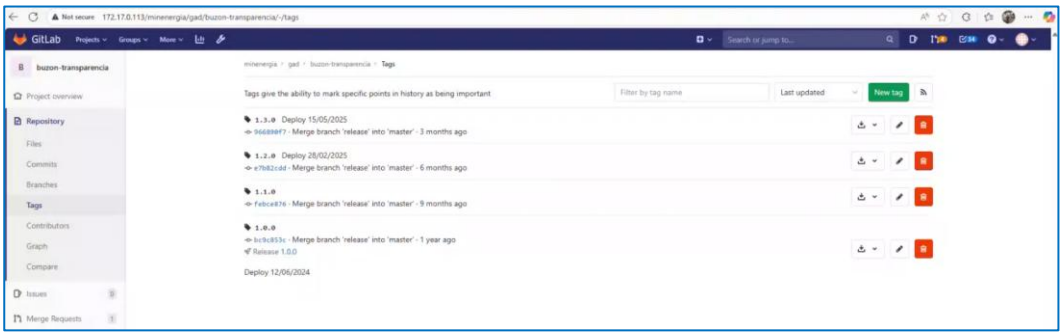
De otra parte, al revisar el versionamiento en la herramienta GITLab se observó que se registra la versión No. 1, lo cual no corresponde con lo identificado en el archivo de despliegue en producción, según se observa en la imagen a continuación:



Al respecto, se confirmó en sesión del 10 de septiembre de 2025, por parte del área auditada que la versión se encuentra desactualizada; sin embargo, el equipo puede verificar la versión a través de los archivos de despliegue.

Para el software Buzón de Integridad

Se observó que el control de versiones se realiza a través de la herramienta GITLab en la que se expuso por parte del área auditada que la ultima versión es la 1.3.0, según se aprecia en la siguiente imagen:



Sin embargo, el numero de la versión no se incluye en el aplicativo, según lo indicado por el área auditada en sesión del 10 de septiembre.

Si bien se indicó adicionalmente que como elemento de control se cuenta con el tag de la rama *“Master”;* no se observa que existan controles que permitan asegurar la trazabilidad de que el software desplegado corresponda a una versión especifica, acorde a la numeración definida en el proyecto o que se visualice el tag de la rama master para poder identificar la versión que fue implementada.

en sesión de auditoría que no se aplican los mismos controles de versionamiento en todos los aplicativos:

En este sentido se observa que (i) no se cuenta con un método estandarizado para asegurar el versionamiento y trazabilidad del software desarrollado y posteriormente

instalado en los ambientes de producción (ii) se evidenció en los casos tomados como muestra que la versión identificada en el sistema GitLab (implementado por el Grupo de Tecnología), no corresponde con la versión del archivo instalador o de despliegue o no se cuenta con un esquema de versionamiento y/o "ramas", lo cual evidencia debilidades en el diseño e implementación de controles obligatorios del MSPI (***A.8.9, A.8.25, A.8.28 y A.8.29),*** así como de los lineamientos para la creación y actualización de la documentación establecidos en el numeral 7.4.3 del documento maestro del MSPI en concordancia con el numeral 7.5.2 de la Norma ISO 27001.

Criterio(s):

Resolución 1519 de 2020 – Anexo 3 - 3.3 PROGRAMACIÓN DEL CÓDIGO FUENTE.

"Los sujetos obligados, en todos sus sitios web, móvil y aplicaciones deberán implementar estándares de desarrollo seguro para evitar vulnerabilidades el código fuente y errores de presentación o alteraciones en el contenido de la información dispuesta al público. Así mismo, se deben evitar mecanismos que puedan poner en riesgo la información o los datos personales o sensibles. Los sujetos obligados deben adoptar las siguientes buenas prácticas: ***1. Realizar análisis estático del código con el objetivo de identificar vulnerabilidades que se encuentra en la programación de las aplicaciones." (Negrita fuera de texto).***

Resolución 02277 de 2021 *""Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia"*

"ARTÍCULO 1*. Actualización del Anexo 1 de la Resolución 500 de 2021. Actualícese el Anexo 1 de la Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", el cual será publicado en la sede electrónica del Ministerio de Tecnologías de la Información y las Comunicaciones, a más tardar quince (15) días siguientes a la expedición de la presente resolución".*

Anexo 1 de la Resolución 02277 - Modelo de Seguridad y Privacidad de la Información:

Numeral 7.4.3. Información documentada del MSPI:
El modelo de seguridad y privacidad de la información de la entidad debe incluir:
• *Información documentada de los lineamientos establecidos.*
• *Documentos que la entidad considere necesarios para la eficacia del SGSI.*
• Reglas claras para crear y actualizar documentos:
identificación, formato, soporte, y control de versiones.
• *La información documentada debe estar disponible y ser adecuada para su uso, donde y cuando se necesite además de estar adecuadamente protegida*

Control A.8.9 Gestión de la configuración

Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.

Control A.8.25 Ciclo de vida de desarrollo seguro del MSPI

Deben establecerse y aplicarse normas para el desarrollo seguro de software y sistemas.

Control A.8.28 Codificación segura del MSPI

Control: Los principios de codificación segura deben aplicarse al desarrollo de software.

Control A.8.29 Pruebas de seguridad y de aceptación en el desarrollo.

Los procesos de pruebas de seguridad deben definirse e implementarse en el ciclo de vida del desarrollo.

Norma ISO 27001
7.5.2 Creación y actualización
Cuando se crea y actualiza información documentada, la organización debe asegurarse de que lo siguiente sea apropiado:
a) la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);
*b) el formato (por ejemplo, idioma, **versión del software**, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);*
c) la revisión y aprobación con respecto a la idoneidad y adecuación.

Posible(s) causa(s) identificada(s) por la Oficina de Control Interno

- *Debilidades en la adopción de lineamientos para la gestión y desarrollo seguro de software en entidades públicas.*
- *Debilidades metodológicas y falta de lineamientos por parte del Grupo TICS para el diseño e implementación de controles de desarrollo acorde al MSPI.*
- *Posible falta de conocimiento y habilidades en materia de gestión del riesgo y diseño de controles por parte de la primera línea de defensa.*

Posible(s) Consecuencias o efectos (s) identificado(s) por la Oficina de Control Interno

- *Posible incumplimiento de disposiciones legales, afectación de la operación por cuenta de riesgos no identificados y/o debilidades en la implementación de controles.*
- *Posible afectación reputacional por la inadecuada gestión de riesgos por parte de la Entidad.*
- *Posible afectación o impacto en la calidad y seguridad de software desarrollado por la Entidad al no aplicar pruebas de código estático.*

Recomendación(nes) específica(s):

- ✓ *Evaluar la pertinencia de relacionar posibles casusas asociadas al riesgo corrupción de manera conjunta con la OPGI y fortalecer los controles y lineamientos para la gestión de riesgos y diseño de controles.*
- ✓ *Evaluar la pertinencia de incluir la descripción del propósito de los controles a fin de tener claramente identificadas las causas que mitigan, en concordancia con los*

lineamientos dados por la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 4, emitida por el DAFP.

- ✓ *Fortalecer las habilidades y competencias del Grupo de Trabajo de Tecnología en materia de gestión de riesgos y diseño de controles.*

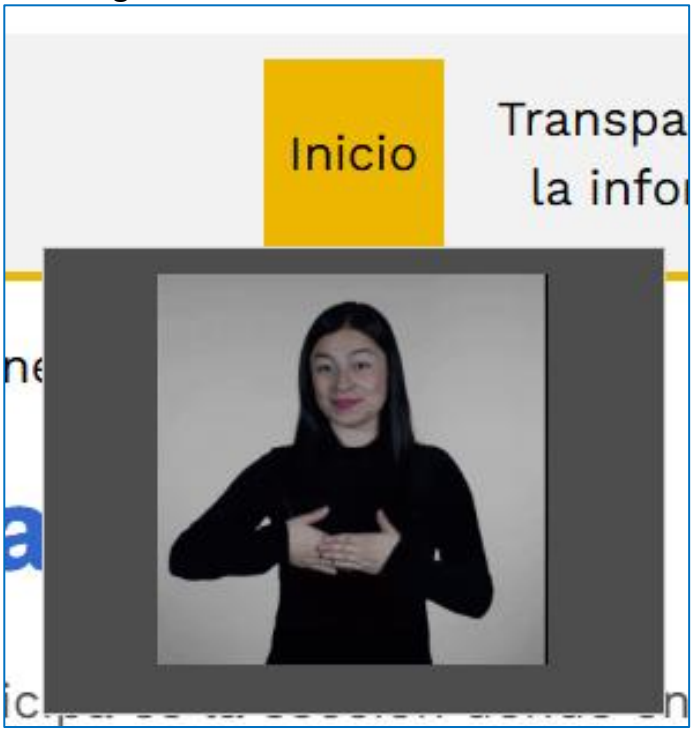
8.4 COMPONENTE INFORMACIÓN Y COMUNICACIÓN

En lo relacionado con el componente de información y comunicación es importante precisar que las páginas web y las sedes electrónicas de las Entidades públicas son activos de información vitales para asegurar la comunicación activa con la ciudadanía y los grupos de valor.

En este sentido y en concordancia con los requisitos planteados por la ley de transparencia (ley 1712 de 2014) y sus directrices para la accesibilidad web (Norma técnica Colombiana NTC 5854), la Oficina de Control Interno verificó los lineamientos de accesibilidad y usabilidad de la página web del ministerio evidenciando que la Entidad ha contemplado condiciones de accesibilidad las cuales se enuncian a continuación:

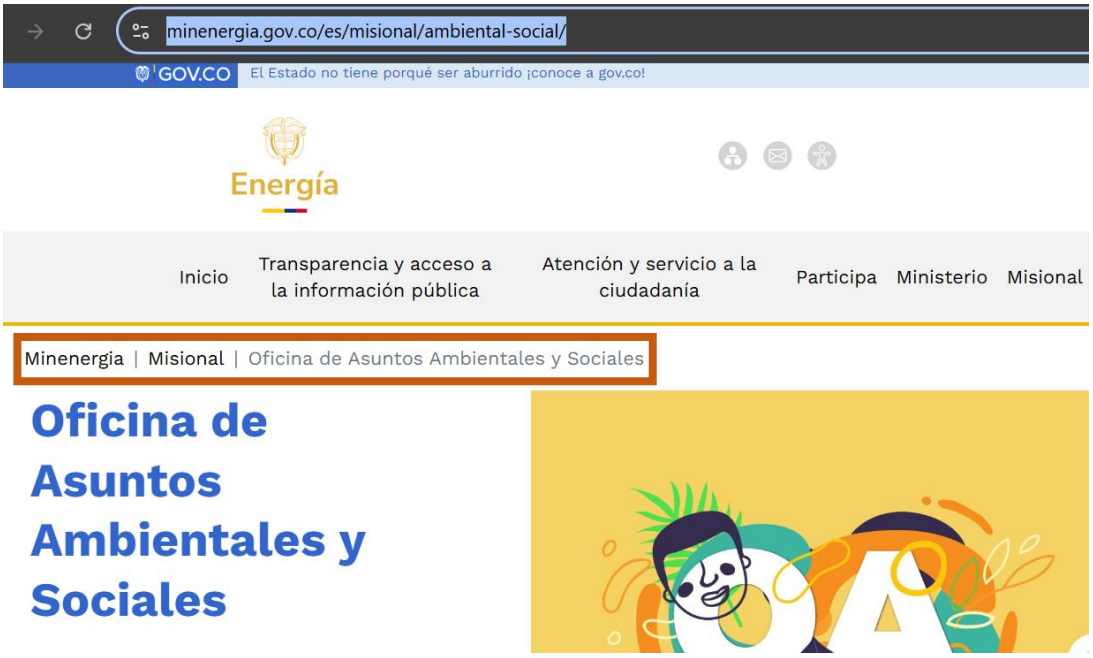
1. **Alternativas textuales a contenidos no textuales:**

Se evidenció que en la página de inicio y menú principal se cuenta con videos descriptivos en lenguaje de señas para los sitios principales del sitio, según se observa en la siguiente imagen:



Ruta de Migas

Se evidenció en el ejercicio auditor que la página web habilita en cada página desplegada la ruta del sitio y permite su navegación para ubicar al usuario en las secciones de su interés y la ruta que ha seguido, según se muestra e la siguiente imagen:

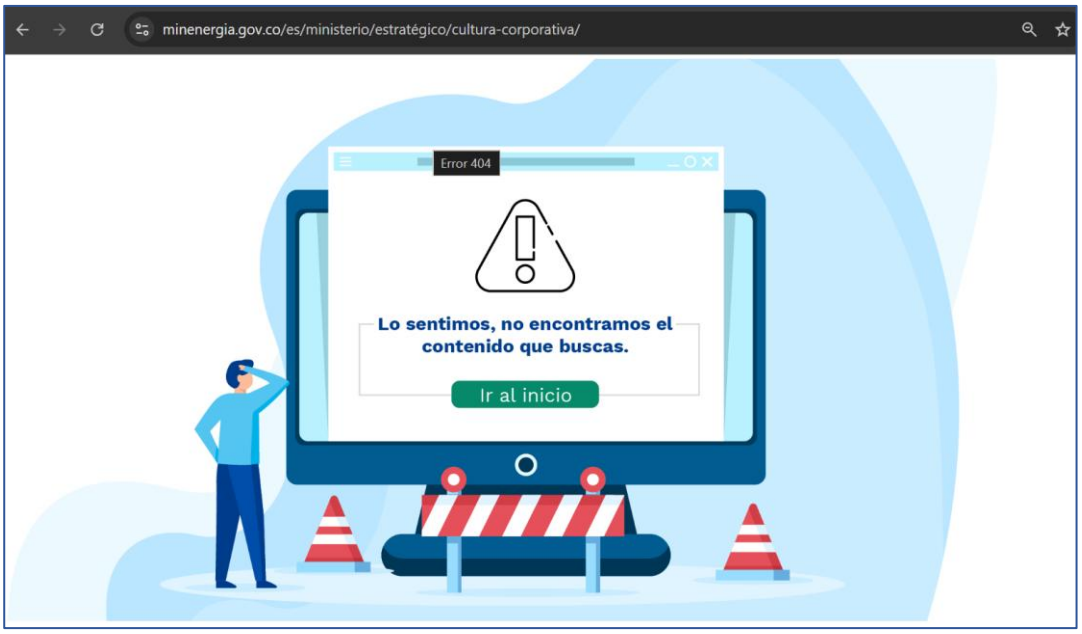


Implementación de subtítulos en videos (Close Caption)

Se evidenció la implementación del sistema close caption o subtítulos como alternativa textual a contenidos audiovisuales (videos), según se presenta en la imagen a continuación:

Manejo de errores:

Se identificó que al navegar la sección de transparencia e ingresar al enlace 1.1, se presentó error de acceso según se evidencia en la siguiente imagen:



En este sentido se observa que en la página web de la Entidad se han definido controles para la presentación de errores a los usuarios.

No obstante lo anterior, al no presentar la información requerida por la ley de transparencia se observan debilidades en la publicación de información mínima requerida en el Anexo 2 de la resolución 1519 de 2020**. (Ver Hallazgo 05).**

De otra parte, con el objetivo de verificar las condiciones técnicas de accesibilidad, se realizó un diagnóstico utilizando la herramienta WAVE (Web Accesibilty Evaluation Tool) la cual puede ser consultada en el enlace https://wave.webaim.org/, a partir de las cuales se identificaron errores y alertas relacionadas con accesibilidad. **(ver hallazgo No 04).**

***HALLAZGO Nº 04* – Incumplimiento de condiciones de Accesibilidad en página web.**

Condición:

Con el objetivo de verificar la implementación de condiciones de accesibilidad en la página web del Ministerio de Minas y Energía, se aplicaron pruebas de diagnóstico de accesibilidad usando la herramienta WAVE (Web Accesibilty Evaluation Tool) la cual puede ser consultada en el enlace https://wave.webaim.org/.

Con el objetivo de presentar los resultados obtenidos, se presentan a continuación los Errores y alertas detectados por la herramienta web indicando el enlace (url) y la imagen de cada sección en la que se aplicaron las pruebas:

Para la url: https://www.minenergia.gov.co/es/ (página de Inicio)

Errores	***Alertas***	***Página web***
42 Errors 13 X Missing alternative text 17 X Linked image missing alternative text 2 X Missing form label 1 X Empty button 9 X Broken ARIA reference	38 Alerts 3 X A nearby image has the same alternative text 2 X Long alternative text 11 X Image with title 3 X Skipped heading level 13 X Redundant link 2 X Link to PDF document 4 X Redundant title text	 *Fuente: Página web.*

Para la url: https://www.minenergia.gov.co/es/ (Sección de transparencia)

Errores	***Alertas***	***Página web***
22 Errors 1 X Missing alternative text 10 X Linked image missing alternative text 1 X Missing form label 1 X Empty button	46 Alerts 1 X Skipped heading level 18 X Redundant link 2 X Link to Excel spreadsheet	 *Fuente: Página web.*

Errores	Alertas	Página web
9 X Broken ARIA reference 3 Contrast Errors 3 X Very low contrast	24 X Link to PDF document 1 X YouTube video	

Para la url: https://www.minenergia.gov.co/es/servicio-al-ciudadano/ (Servicio al Ciudadano)

Errores	Alertas	Página web
19 Errors 10 X Linked image missing alternative text 1 X Missing form label 1 X Empty button 7 X Broken ARIA reference 4 Contrast Errors 4 X Very low contrast	66 Alerts 3 X Skipped heading level 9 X Redundant link 3 X Link to Excel spreadsheet 48 X Link to PDF document 3 X YouTube video	 *Fuente: Página web.*

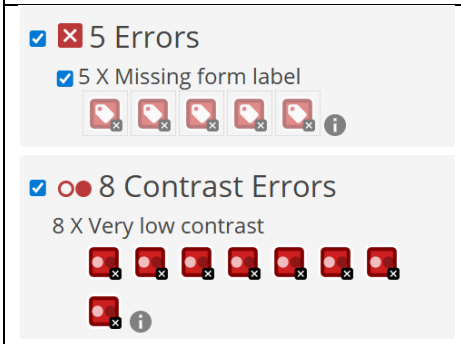
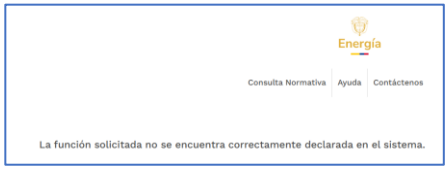
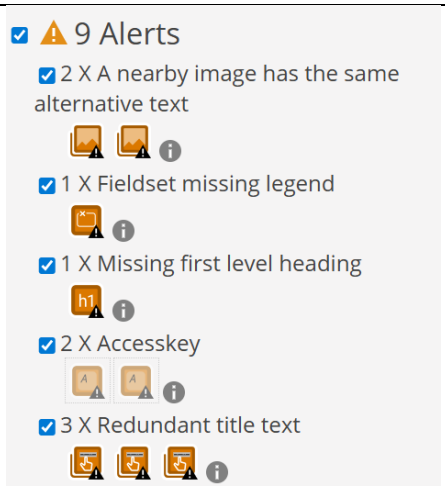
Para la url: https://www.minenergia.gov.co/es/participa/ (Participa)

Errores	Alertas	Página web
17 Errors 10 X Linked image missing alternative text 1 X Missing form label 1 X Empty button 5 X Broken ARIA reference 2 Contrast Errors 2 X Very low contrast	12 Alerts 1 X Skipped heading level 9 X Redundant link 2 X YouTube video	 *Fuente: Página web.*

Para la url: https://www.minenergia.gov.co/es/misional/ (Misional)

Errores	Alertas	Página web
14 Errors 1 X Missing alternative text 10 X Linked image missing alternative text 1 X Missing form label 1 X Empty button 10 Contrast Errors 10 X Very low contrast	19 Alerts 1 X Long alternative text 1 X Skipped heading level 1 X Possible heading 9 X Redundant link 7 X Justified text	 *Fuente: Página web.*

Para la url: https://normativame.minenergia.gov.co/loader.php?lServicio=Normatividad&lTipo=User&lFuncion=buscar (Normativa)

Errores	***Alertas***	***Página web***
 *La página inicia el cague de información mostrando lo siguiente:*  *Sin embargo, un segundo después muestra el siguiente mensaje:*  *Lo anterior representa un error de navegación toda vez que no muestra el mensaje de error estándar y adicionalmente no muestra el contenido ni imagen institucional.*		 *Fuente: Página web.*

Para la url: https://normativame.minenergia.gov.co/loader.php?lServicio=Normatividad&lTipo=User&lFuncion=buscar (Normativa)

Errores	***Alertas***	***Página web***
20 Errors 5 X Missing alternative text 10 X Linked image missing alternative text 2 X Missing form label 1 X Empty button 2 X Broken ARIA reference 15 Contrast Errors 15 X Very low contrast	17 Alerts 1 X Skipped heading level 9 X Redundant link 3 X HTML5 video or audio 4 X YouTube video	 *Fuente: Página web.*

Para la url: https://www.minenergia.gov.co/es/misional/energia-electrica-2/ (Misional – Energía eléctrica)

Errores	Alertas	Página web
13 Errors 10 X Linked image missing alternative text 1 X Missing form label 1 X Empty button 1 X Broken ARIA reference 2 Contrast Errors 2 X Very low contrast	20 Alerts 1 X Skipped heading level 9 X Redundant link 9 X Justified text 1 X YouTube video	 *Fuente: Página web.*

Para la url: https://www.minenergia.gov.co/es/misional/hidrocarburos/ (Misional – Hidrocarburos)

Errores	Alertas	Página web
15 Errors 2 X Missing alternative text 10 X Linked image missing alternative text 1 X Missing form label 1 X Empty button	15 Alerts 1 X Skipped heading level 9 X Redundant link 2 X Link to PDF document 3 X Justified text	 *Fuente: Página web.*

Errores	Alertas	Página web
1 X Broken ARIA reference 6 Contrast Errors 6 X Very low contrast		

Para la url: https://www.minenergia.gov.co/es/misional/ambiental-social/ (Misional – Oficina de Asuntos Ambientales y Sociales)

Errores	Alertas	Página web
13 Errors 10 X Linked image missing alternative text 1 X Missing form label 1 X Empty button 1 X Broken ARIA reference 2 Contrast Errors 2 X Very low contrast	10 Alerts 1 X Skipped heading level 9 X Redundant link	

Fuente: Página web.

Los errores anteriormente descritos en cada una de las secciones analizadas evidencian el incumplimiento de lineamientos del Anexo 1 “Directrices de accesibilidad web”, de la resolución 1519 de 2020.

Criterio(s):

Resolución 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”.*

Anexo 1 - Directrices de accesibilidad web

"2.2.3.1 Alternativas a lo sensorial.

CC1. Alternativa texto para elementos no textuales. *Elementos estáticos como fotografías, imágenes, diagramas, mapas y similares, como también, los sonidos cortos de alerta, vibraciones u otros que constituyan elementos no textuales, deben indispensablemente llevar un texto alternativo que cumpla con el mismo propósito que este elemento tiene para quienes lo pueden ver, escuchar o sentir.*

CC5. Contraste de color suficiente en textos e imágenes. *El contraste de color, de forma general, debe estar dado por colores de textos e imágenes cuyos fondos sean oscuros si los colores originales son claros, o viceversa. Ello garantiza contraste suficiente para visibilizar los textos y gráficos. Los contrastes no deben ser de textos totalmente claros sobre fondos totalmente oscuros o viceversa, ya que todo sería blanco sobre negro o de contrastes similares. El contraste de los colores debe permitir la visualización sin dificultad.*

CC7. Identificación coherente*. Se hace indispensable que las opciones, enlaces o elementos que realicen las mismas acciones o lleven a los mismos sitios específicos, se muestren de la misma forma y con el mismo aspecto visual y textual. Ejemplo. Un enlace "Contáctenos" más otro enlace "Contacte con nosotros" no deben llevar al mismo sitio, ya que no son iguales, si llevaran al mismo sitio necesariamente, debería asumir el texto y el aspecto visual del primero o del segundo, pero ser iguales en todo caso. Si, por el contrario, dos enlaces "Contáctenos" llevaran uno a la Subdirección Técnica y el otro a Atención al Ciudadano, deberían ser distinguibles adecuadamente, por ejemplo, como "Contacte con la Subdirección Técnica" y "Contacte con la oficina de Atención al Ciudadano".*

Posible(s) causa(s) identificada(s) por la Oficina de Control Interno

- Desconocimiento de lineamientos dados por el anexo 2 de la resolución 1519 de 2020.
- Posible Replicación de elementos (secciones, botones, imágenes) al momento de crear secciones y micrositios sin verificar su aplicabilidad y accesibilidad.
- Posibles debilidades en la ejecución de diagnósticos de accesibilidad en la página web de la Entidad.

Posible(s) Consecuencias o efectos (s) identificado(s) por la Oficina de Control Interno

- Inadecuada trazabilidad de publicación de registros de información de la Entidad.
- Posible afectación reputacional por el incumplimiento de lineamientos de la ley de transparencia y la resolución 1519 de 2020.

Recomendación(nes) específica(s):

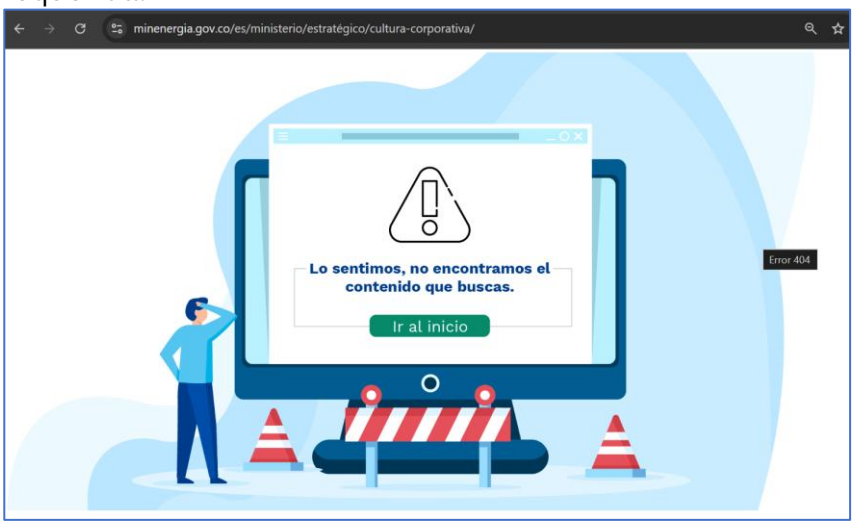
- Fortalecer el conocimiento del Grupo de Comunicaciones y Prensa en lo relacionado con los lineamientos de la Resolución 1519 de 2020 y sus anexos.
- Definir lineamientos y condiciones de publicación de contenidos de la Sección de transparencia, teniendo en cuenta los lineamientos descritos en el numeral 2.4.1 Criterios generales de publicación de información pública del anexo 2 de la resolución 1519 de 2020, relacionados con la información publicada en la sección de Transparencia de la Entidad.

***HALLAZGO Nº 05* – Debilidades en la aplicación del estándar de publicación de información mínima**

Condición:

Con el objetivo de verificar el cumplimiento del cumplimiento del anexo 2 de la resolución 1519 de 2020 "Estándar de publicación", se realizó verificación de una muestra de los enlaces de la sección de transparencia encontrando lo siguiente:

1. Enlaces que reportan mensaje de error y no muestran la información mínima requerida:



Se evidenció que se presenta página de error en los siguientes enlaces:

"1.1 Misión y Visión"
(enlace: https://www.minenergia.gov.co/es/ministerio/estrat%C3%A9gico/cultura-corporativa/)
"1.2Funciones y Deberes:"
(enlace: https://www.minenergia.gov.co/es/ministerio/estructura-organizacional/funciones/)

"2.1.2 Decreto único reglamentario:"
(enlace: https://www.minenergia.gov.co/es/repositorio-normativo/decretos-modificatorios-al-decreto-%C3%BAnico-reglamentario-del-sector-administrativo-de-minas-y-energ%C3%ADa/)
"2.1.5.1 Políticas y lineamientos sectoriales:"
(enlace: https://www.minenergia.gov.co/es/ministerio/estrat%C3%A9gico/planes-y-programas/#planes-programas)
"5. Trámites y Servicios:"
(enlace: https://www.minenergia.gov.co/es/servicio-al-ciudadano/tr%C3%A1mites-y-servicios/)

Criterio(s):

Resolución 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".*
Anexo 2 - Estándares de publicación y divulgación información

"2.4.2 Menú de Transparencia y acceso a la información pública:

(...) Estandarización de contenidos

Los sujetos obligados estandarizarán la estructura de contenidos para la divulgación de información pública. Las personas naturales y jurídicas referidas en el los literales c), d), f), g) del artículo 5 de la Ley 1712 del 2014, publicarán la información que se produzca en relación con el ejercicio de la función pública, servicio público, ejercicio de autoridad, o sobre fondos públicos que reciban o intermedien, y a las que la normativa vigente les obligue. La siguientes es la estructura de contenidos del menú de transparencia y acceso a la información:

(...) 1.1 Misión, visión, funciones y deberes. De acuerdo con la normativa que le aplique y las definiciones internas, incluyendo norma de creación y sus modificaciones. (....)

(...) 2.1.2 Decreto Único Reglamentario. (...)

(...) 2.1.5 Políticas, lineamientos y manuales. Cada sujeto obligado deberá publicar sus políticas, lineamientos y manuales, tales como, según le aplique: (a) Políticas y lineamientos sectoriales;(...)

(...) 5. Trámites En esta sección encontrará información de los Trámites (...).

Posible(s) causa(s) identificada(s) por la Oficina de Control Interno

- Posible Desconocimiento de lineamientos dados por el anexo 2 de la resolución 1519 de 2020.
- Inadecuada trazabilidad de publicación de registros de información de la Entidad.

Posible(s) Consecuencias o efectos (s) identificado(s) por la Oficina de Control Interno

- Afectación reputacional por incumplimiento de las disposiciones legales de la ley de transparencia y la resolución 1519 de 2020.
- Posible afectación en la medición del desempeño de la Entidad a traves del Indicador de Transparencia y Acceso a la Información – ITA a cargo de la Procuraduría General de la Nación.

Recomendación(nes) específica(s):

- Fortalecer el conocimiento del Grupo de Comunicaciones y Prensa y del Grupo TICS en lo relacionado con los lineamientos de la Resolución 1519 de 2020 y sus anexos.
- Definir lineamientos y condiciones de publicación de contenidos de la Sección de transparencia, teniendo en cuenta los lineamientos descritos en el numeral 2.4.2 “Menú de Transparencia y acceso a la información pública” del anexo 2 de la resolución 1519 de 2020, relacionados con la información publicada en la sección de Transparencia de la Entidad.

***HALLAZGO Nº 06* - Información de la Entidad sin fecha de publicación en la página web**

Condición:

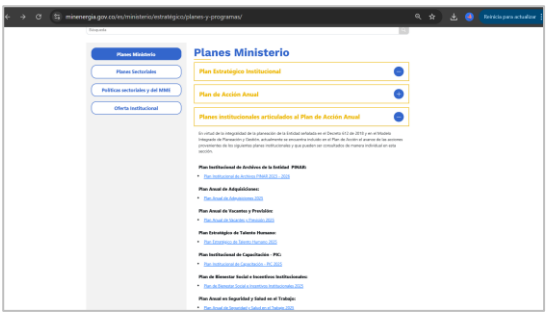
Se observa en primera instancia que el proceso es responsable de la gestión de los planes (i)Plan estratégico de Tecnologías de la Información – PETI, (ii) Plan de tratamiento de riesgos de seguridad de la información y (iii) Plan de seguridad y privacidad de la información, definidos como información mínima requerida por la ley 1712 de 2014 (ley de transparencia), en este sentido se verificó que dichos planes se encontraran publicados en la sección de transparencia de la Entidad en articulación con el Plan de acción como se pudo evidenciar en el link: https://www.minenergia.gov.co/es/ministerio/estrat%C3%A9gico/planes-y-programas/

También se evidenció que los mencionados planes fueron aprobados en sesión del comité Institucional de Gestión y Desempeño el día 28 de enero de 2025.

Para la vigencia 2024:

En la misma sección se dispone de un botón “Años Anteriores” el cual permite la consulta histórica de los planes anteriormente mencionados.

No obstante lo anterior, en la página web no se referencia la fecha de publicación de la Información, según puede apreciarse en las siguientes imágenes:



Plan Estratégico de Tecnología de la Información y las Comunicaciones – PETI:

- Plan Estratégico de Tecnología de la Información y las Comunicaciones – PETI 2024-2027

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información:

- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025
- Seguimiento Primer Trimestre - Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025

Plan de Seguridad y Privacidad de la Información:

- Plan de Seguridad y Privacidad de la Información 2025
- Seguimiento Primer Trimestre - Plan de Seguridad y Privacidad de la Información 2025

Fuente: Página Web de la Entidad

Así mismo, dentro de la sección de transparencia se encontraron distintos tipos de información publicada sin que se indique la fecha de publicación, según se muestra en las siguientes imágenes:

3.1 Plan Anual de Adquisiciones

7 Datos Abiertos (registro de Activos de Información y Esquema de publicación de Información)

Lo anterior incumple el literal e) del numeral 2.4.1 Criterios generales de publicación de información pública del anexo 2 de la resolución 1519 de 2020, el cual indica:

"Todo documento o información debe indicar la fecha de su publicación en página web".

Criterio(s):

Resolución 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".*
Anexo 2 - Estándares de publicación y divulgación información

"2.4.1 Criterios generales de publicación de información pública:

(...) e. Todo documento o información debe indicar la fecha de su publicación en página web.

Posible(s) causa(s) identificada(s) por la Oficina de Control Interno

- Desconocimiento de lineamientos dados por el anexo 2 de la resolución 1519 de 2020.

Posible(s) Consecuencias o efectos (s) identificado(s) por la Oficina de Control Interno

- Inadecuada trazabilidad de publicación de registros de información de la Entidad.

Recomendación(nes) específica(s):

- Fortalecer el conocimiento del Grupo de Comunicaciones y Prensa en lo relacionado con los lineamientos de la Resolución 1519 de 2020 y sus anexos.
- Definir lineamientos y condiciones de publicación de contenidos de la Sección de transparencia, teniendo en cuenta los lineamientos descritos en el numeral 2.4.1 Criterios generales de publicación de información pública del anexo 2 de la resolución 1519 de 2020, relacionados con la información publicada en la sección de Transparencia de la Entidad.

8.5 COMPONENTE ACTIVIDADES DE MONITOREO

La verificación del presente componente se llevó a cabo teniendo en cuenta los lineamientos y directrices emitidos por el Ministerio de Minas y Energía, con la finalidad de identificar la eficacia en la aplicación de controles y actividades de monitoreo a partir de los indicadores definidos para el sistema de gestión de seguridad de la información, así como los aspectos relacionados con el seguimiento a los planes de tratamiento de riesgos y las revisiones periódicas por parte de la dirección en concordancia con los lineamientos emitidos por MinTIC para la Gestión de Seguridad de la Información en el marco de implementación del Modelo de Seguridad y Privacidad de la Información – MSPI.

HALLAZGO Nº 7 - Incumplimiento en la medición del Desempeño del Sistema de Gestión de Seguridad de la Información

Condición:

Se identificó en primera instancia que el Ministerio de Minas y Energía ha adoptado políticas de seguridad de la información y según la documentación aportada por el Grupo de Tecnología de la Información y las Comunicaciones, a través del documento "MINENERGÍA_Indicadores de Gestión para el MSPI_03032022_V_1.0.pdf" se definieron los siguientes indicadores de desempeño:

- Indicador de Sensibilización.
- Indicador de Ataques Informáticos.
- Indicador de privacidad y confidencialidad.
- Indicador de Incidentes
- Indicador de Implementación de Controles
- Indicador de Riesgos
- Indicador de efectividad en capacitaciones del SGSI.

En el mencionado también se definen distintos atributos de los indicadores en mención, tales como: formula, descripción, periodicidad de medición entre otros, que dan cuenta del diseño de instrumentos de medición del desempeño de la Gestión de Seguridad de la Información; sin embargo según se confirmó por parte del área auditada, en sesión de auditoría del 8 de septiembre de 2025, no se cuenta con el registro de medición de dichos indicadores, de manera que no fue posible observar el comportamiento histórico de los indicadores como insumo para la gestión estratégica de seguridad de la información y la medición del desempeño del MSPI.

Situación que incumple los lineamientos dados en el numeral 9.1. Seguimiento, medición, análisis y evaluación del Modelo de Seguridad y Privacidad de la Información y los lineamientos generales de implementación de la 4ª. Dimensión: "Evaluación de Resultados", del Modelo Integrado de Planeación y Gestión - MIPG.

Criterio(s):

Resolución 02277 de 2021 *"Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia"*

"ARTÍCULO 1*. Actualización del Anexo 1 de la Resolución 500 de 2021. Actualícese el Anexo 1 de la Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", el cual será publicado en la sede electrónica del Ministerio de Tecnologías de la Información y las Comunicaciones, a más tardar quince (15) días siguientes a la expedición de la presente resolución".*

Anexo 1 de la Resolución 02277 - Modelo de Seguridad y Privacidad de la Información:

9. Fase 3: Evaluación de desempeño

Una vez culminada las actividades de la fase de operación del MSPI, se evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 "Protección de datos personales", Ley 1712 de 2014 "Ley de Transparencia y Acceso a la Información Pública", Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue."

9.1. Seguimiento, medición, análisis y evaluación

"Las entidades deben conocer sus avances en la implementación del modelo de Gobierno Digital, estableciendo tiempos y recursos para su monitoreo y reporte ante el Comité de Gestión y Desempeño, conforme al MIPG
Es importante incluir dentro del plan de auditorías los temas relacionados con seguridad digital como lo establece el MIPG.
Los mecanismos utilizados para medir, analizar, monitorizar, evaluar y realizar seguimiento a la eficacia del Sistema deben ser comparables y reproducibles"

Modelo Integrado de Planeación y Gestión (MIPG) Dimensión 4: **Evaluación de Resultados**

"Lineamientos generales para la implementación

(...) Evaluar el logro de los resultados
Para ello, se debe aplicar los indicadores definidos de acuerdo con las decisiones que la entidad haya asumido y las disposiciones establecidas en las normas y lineamientos de política frente a las maneras, plazos y poblaciones a quienes decide entregar la información del seguimiento y evaluación (...)

Posible(s) causa(s) identificada(s) por la Oficina de Control Interno

- Debilidades en la adopción de herramientas de medición del desempeño de seguridad.
- Falta de adopción de buenas prácticas de gestión de seguridad de la información.
- Debilidad en la apropiación de conocimientos y habilidades para la medición del desempeño de seguridad de la información.
- Debilidad en el seguimiento y control de indicadores de seguridad de la Información diseñados.

Posible(s) Consecuencias o efectos (s) identificado(s) por la Oficina de Control Interno

- Inadecuado tratamiento de riesgos oportunidades de seguridad de la información.
- Posible afectación a la toma de decisiones estratégicas en materia de seguridad de la información por desconocimiento del comportamiento de los indicadores.

Recomendación(nes) específica(s):

- Aplicar evaluaciones del modelo de madurez en la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI así como del Modelo de Referencia de Arquitectura Empresarial y sus componentes.
- Adoptar las recomendaciones de la guía "Lineamientos de Indicadores de Gestión de Seguridad de la Información" versión 5, del 21 de abril de 2025 (https://gobiernodigital.mintic.gov.co/692/articles-401772_recurso_1.pdf).
- Adelantar los tramites internos de formalización de procedimientos dentro del SIG, de manera articulada con la OPGI.
- Evaluar la pertinencia de articular la medición del desempeño e indicadores asociados al sistema de gestión de seguridad de la información dentro del Sistema Integrado de Gestión – SIG, del Ministerio de Minas y Energía.

***HALLAZGO Nº 8* – Debilidades en la revisión por la Dirección**

Condición:

En atención al requerimiento de información relacionado con las actas de revisión por la dirección se aportaron los siguientes documentos:

- Acta_No.3_Comite__de_Coordinaciòn_del_Sistema_de_Control_Interno_26112024_1 (1).pdf
- *Acta_sesion1_CIGD_2025.pdf*

A partir de lo anterior es preciso tener en cuenta que acorde a lo establecido en el Modelo de Seguridad y Privacidad de la Información, el propósito de la revisión por la Dirección es:

"Revisar el MSPI de la entidad, por parte de la alta dirección (comité Institucional de Gestión y Desempeño), en los intervalos planificados, que permita determinar su conveniencia, adecuación y eficacia".

De otra parte, es importante tener en cuenta lo definido por la Norma ISO 27001 en lo relacionado con el numeral 9.3.2 *"Entradas para la revisión por la dirección"* , el cual establece:

"La revisión por la dirección debe incluir:
a. El estado de las acciones de las revisiones por la dirección previas;
b. Cambios en los aspectos externos e internos que son relevantes para el SGSI de la información;
c. Cambios en las necesidades y expectativas de las partes interesadas que son relevantes para el SGSI de la información;
d. Retroalimentación del desempeño de la seguridad de la información, incluyendo tendencias en:
1. No conformidades y acciones correctivas;
2. Resultados del seguimiento y la medición;
3. Resultados de auditoría;

4. Cumplimiento de los objetivos de la seguridad de la información;
e. Retroalimentación de las partes interesadas;
f. Resultados de la evaluación de riesgos y estado del plan de tratamiento de riesgos;
g. Oportunidades de mejora continua."

En este sentido se observa que aunque en el desarrollo del Comité de Coordinación de Control Interno se evalúan algunos aspectos de manera general a nivel de control interno, no se abordan aspectos específicos del funcionamiento, implementación, diseño de controles, gestión de riesgos, indicadores entre otros, aplicables al Sistema de Gestión de Seguridad de la información en específico, por tanto, no se puede entender que el soporte "Acta_No.3_Comite__de_Coordinaciòn_del_Sistema_de_Control_Interno_26112024_1 (1).pdf", entregado por el Grupo de Tecnología, corresponda a la "Revisión por la Dirección", toda vez que, no se desarrolla en la instancia definida por el MSPI y no aborda aspectos específicos del Sistema de Gestión de Seguridad de la Información.

Adicionalmente, acorde a los resultados de la presente auditoría, se evidenciaron desviaciones en (i) el registro y seguimiento de indicadores de seguridad de la información y (ii) la aplicación de controles de aprobación de documentos por parte del CIGD, requeridos por el MSPI como son la "declaración de aplicabilidad", el "compendio de requisitos de las partes interesadas" y la falta de evidencia de aprobación del manual del sistema de gestión de seguridad de la información aportado por el área auditada, **(Ver Hallazgo Nº 1 – Incumplimiento en la Identificación de Requisitos de las Partes Interesadas),** lo que inherentemente implica que no se han tenido en cuenta aspectos ("entradas") necesarias para la revisión por parte de la dirección relacionados con:

a. El estado de las acciones de las revisiones por la dirección previas;
b. Cambios en los aspectos externos e internos que son relevantes para el SGSI de la información;
c. Cambios en las necesidades y expectativas de las partes interesadas que son relevantes para el SGSI de la información;
d. Retroalimentación del desempeño de la seguridad de la información, incluyendo tendencias en:
(...) 2. Resultados del seguimiento y la medición; (...)

Así como las entradas definidas por el Modelo de Seguridad y Privacidad de la Información en lo relacionado con:

Los documentos de alto nivel del MSPI deberán ser aprobados, incluyendo los actos administrativos que se necesiten para constituirlos al interior de la entidad.

En este sentido se observa incumplimiento del numeral 9.3. *"Revisión por la dirección"* del MSPI y los lineamientos del numeral 9.3.2 *"Entradas para la revisión por la dirección"* de la Norma ISO 27001.

De otra parte, frente al documento *"Acta_sesion1_CIGD_2025.pdf"*, se observa que corresponde a una sesión del Comité Institucional de Gestión y Desempeño, sin embargo,

según se observa en la siguiente imagen tomada del documento y correspondiente al orden del día:

ORDEN DEL DÍA

	TEMA	RESPONSABLE	PROPÓSITO
1	REVISIÓN QUORUM E INTRODUCCIÓN	Of. De Planeación y Gestión Internacional, OPGI - Miguel Cardozo	CONTEXTO
2	MISIÓN, VISIÓN	Despacho de Ministro, Equipo de Análisis Estratégico – Martha Bernal	**APROBACIÓN**
3	PLAN DE ACCIÓN ANUAL 2025	OPGI - Miguel Cardozo	**APROBACIÓN**
4	PLANES INSTITUCIONALES		
	4.1 PLANES DE TALENTO HUMANO:	Subdirección de Talento Humano – Sandra Milena Rodríguez	**APROBACIÓN**
	Plan Estratégico de Talento Humano Plan de Capacitación Plan de Bienestar Social e Incentivos Plan de Previsión y Vacantes Plan de Seguridad y Salud en el Trabajo		
	4.2 PLANES DE TECNOLOGÍA	Secretaría General, Grupo de Tecnologías de la Información y las Comunicaciones - Leidy Galindo	**APROBACIÓN**
	Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información Plan de Seguridad y Privacidad de la Información		
	4.3 PLAN INSTITUCIONAL DE ARCHIVOS - PINAR	Secretaría General, Grupo de Relacionamiento con el Ciudadano y Gestión de la Información – Jenny Nova	**APROBACIÓN**
	4.4 PLAN DE AUSTERIDAD	Secretaría General – Leandra Maydeth Durán Cortés	INFORMATIVO
	4.5 PROGRAMA DE TRANSPARENCIA Y ÉTICA PÚBLICA	OPGI - Aida Marcela Nieto P.	INFORMATIVO

Fuente: Acta_sesion1_CIGD_2025.pdf aportada por el Grupo TIC's

Se observa que la sesión tiene como propósito la aprobación de los planes de los que trata el artículo 612 de 2018 y su aprobación por parte del CIGD, mas no aborda los elementos "entradas" para la revisión por parte de la dirección mencionadas anteriormente.

Por otro lado, a pesar de que se mencionaron aspectos relacionados con la planeación de la sesión del Comité Institucional de Gestión de Desempeño, no se identificaron lineamientos y/o planeación de la periodicidad con la que se realiza la "Revisión por la Dirección" así como tampoco se evidenció que se hayan generado las salidas de la actividad de revisión por parte de la Dirección relacionadas con:

- Revisión a la implementación.
- Acta y documento de Revisión por la Dirección.
- Compromisos de la Revisión por la Dirección.

Así las cosas, teniendo en cuenta todo lo expuesto anteriormente, se evidencia el incumplimiento del lineamiento, propósito y salidas de la "Revisión por la Dirección" establecidas en el numeral *"9.3. Revisión por la dirección"*.

Criterio(s):

Resolución 02277 de 2021 *""Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia"*

"ARTÍCULO 1*. Actualización del Anexo 1 de la Resolución 500 de 2021. Actualícese el Anexo 1 de la Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", el cual será publicado en la sede electrónica del Ministerio de Tecnologías de la Información y las Comunicaciones, a más tardar quince (15) días siguientes a la expedición de la presente resolución".*

Anexo 1 de la Resolución 02277 - Modelo de Seguridad y Privacidad de la Información:

"9.3. Revisión por la dirección":

Lineamiento: La Política y el Manual de Seguridad y Privacidad deben ser revisados y aprobados por el Comité de Gestión y Desempeño o por decisión del nominador, considerando los cambios en las necesidades de las partes interesadas.

Propósito: Revisar el MSPI de la entidad, por parte de la alta dirección (comité Institucional de Gestión y Desempeño), en los intervalos planificados, que permita determinar su conveniencia, adecuación y eficacia.

Salidas: • Revisión a la implementación, • Acta y documento de Revisión por la Dirección, • Compromisos de la Revisión por la Dirección

Norma ISO 27001 numeral 9.3.2 "Entradas para la revisión por la dirección"

"La revisión por la dirección debe incluir:
a. El estado de las acciones de las revisiones por la dirección previas;
b. Cambios en los aspectos externos e internos que son relevantes para el SGSI de la información;
c. Cambios en las necesidades y expectativas de las partes interesadas que son relevantes para el SGSI de la información;
d. Retroalimentación del desempeño de la seguridad de la información, incluyendo tendencias en:
1. No conformidades y acciones correctivas;
2. Resultados del seguimiento y la medición;
3. Resultados de auditoría;
4. Cumplimiento de los objetivos de la seguridad de la información;
e. Retroalimentación de las partes interesadas;
f. Resultados de la evaluación de riesgos y estado del plan de tratamiento de riesgos;
g. Oportunidades de mejora continua."

Posible(s) causa(s) identificada(s) por la Oficina de Control Interno

- Desconocimiento de lineamientos dados por el Documento Maestro del MSPI.
- Debilidades en el asesoramiento a la alta dirección para la revisión, seguimiento y evaluación del Sistema de Gestión de Seguridad de la Información
- Falta de aprobación de documentos y lineamientos internos de seguridad de la Información requeridos por el MSPI.

Posible(s) Consecuencias o efectos (s) identificado(s) por la Oficina de Control Interno

- Afectación a la toma de Decisiones por parte de la Dirección en lo relacionado con la gestión de riegos, medición del desempeño e implementación de controles de seguridad de la información del Ministerio de Minas y Energía.
- Posible afectación a la disponibilidad, integridad y confidencialidad de activos de información debido a la ausencia de registro de indicadores y seguimiento al desempeño de controles de seguridad de la información

Recomendación(nes) específica(s):

- Evaluar la pertinencia de definir y documentar los lineamientos de planificación y periodicidad de la “Revisión por la Dirección” (anual, semestral, etc).
- Evaluar la pertinencia de incluir en el orden del día, presentación y demás documentos que evidencien las sesiones de Revisión por la dirección para el sistema de gestión de seguridad de la información, las entradas (temas) definidos en el numeral 9.3.2 de la norma ISO 27001.
- Evaluar la pertinencia de identificar claramente las sesiones del Comité Institucional de Gestión y Desempeño que corresponden a la revisión por la dirección, así como las actas asociadas.
- Concientizar y asesorar a la alta dirección y miembros del CIGD frente a los roles y responsabilidades en relación con la seguridad de la información, atendiendo lo establecido en el numeral 7 del artículo *6. “La gestión de la seguridad de la información, seguridad digital y la gestión de riesgos de la entidad.”,* de la resolución 500 de 2021, el cual establece:

  “Asesorar a la dirección de la entidad sobre seguridad de la información y seguridad digital para que pueda hacer seguimiento y tomar las decisiones adecuadas en esta materia”.
- Evaluar la pertinencia de articular la revisión por la dirección y otros requerimientos transversales a los sistemas de gestión como son alcance, contexto, partes interesadas, recursos, revisión por la dirección, entre otros, del sistema de gestión de seguridad de la información dentro del Sistema Integrado de Gestión – SIG, del Ministerio de Minas y Energía.

***HALLAZGO Nº 9* – Debilidades en la implementación de acciones de mejora**

Condición:

En el desarrollo de la auditoría en lo relacionado con los controles aplicables a la continuidad de negocio la recuperación ante desastres se identificó la acción de mejora identificada con código PM-23-AI2023-07, sin embargo, acorde a lo informado porla Oficina de Planeación y Gestión Internacional – OPGI, teniendo en cuenta que las acciones propuestas relacionadas con:

"1. Identificar los riesgos inherentes del Subproceso Recuperación de Desastres Tecnológicos, y registrarlos en el Mapa de Riesgos del Proceso de Gestión Tecnológica, de Información y Comunicación, liderado por el Grupo de Tecnologías de la Información y las Comunicaciones – GTICS".
"2. Identificar los riesgos inherentes del Subproceso Continuidad de Negocio, y registrarlos en el Mapa de Riesgos del Proceso de Gestión Tecnológica, de Información y Comunicación, liderado por el Grupo de Tecnologías de la Información y las Comunicaciones - GTICS.

tenían como fecha máxima para su cumplimiento el 29 de diciembre de 2023 y después de múltiples comunicaciones por parte de la OPGI, no se ha reportado el cumplimiento de las acciones propuestas, según se observa en correo del 2 de julio de 2025, en el cual se indica frente a la acción PM-23-AI2023-07:

"(...) Agradezco igualmente el respaldo del área, teniendo en cuenta que este plan corresponde al año 2023 y, a la fecha, no se ha logrado avanzar en la ejecución de las acciones establecidas o la evidencia de las acciones no ha sido reportada a nuestro grupo. (...)"

En este sentido, la Oficina de Control Interno requirió mediante correo electrónico del pasado 11 de septiembre, confirmación al área auditada respecto a los siguientes temas relacionados:

"Acorde a lo verificado con la OPGI, se observa que a la fecha no se ha solicitado reformulación y/o se ha reportado el cumplimiento de la Acción de Mejora identificada con el código PM-23-AI2023.

En este sentido, solicito su colaboración para confirmar por este medio lo siguiente:

1. Confirmar la fecha en la que se remitieron los soportes de cumplimiento a la OPGI, adjuntando las evidencias respectivas (archivos, correos, memorandos, etc). en caso de no contar con estos soportes indicarlo de manera escrita por este medio.

2. Confirmar la fecha en la que se realizó la reformulación del plan de mejoramiento, adjuntando las evidencias respectivas (archivos, correos, memorandos, etc). en caso de no contar con estos soportes indicarlo de manera escrita por este medio.

3. A partir de lo expuesto en sesión de auditoría, se indicó que la metodología de riesgos se encuentra en proceso de actualización, por lo que solicito me confirmen el código de acción/plan de mejoramiento, asociada a esta actividad de mejora, adjuntando el formato de formulación de acción correspondiente. en caso de no contar con estos soportes y/o registro de formulación de plan de mejoramiento, indicarlo de manera escrita por este medio".

Sin embargo, con corte al 19 de septiembre no se recibió, respuesta al requerimiento de información.

En este sentido se evidencia incumplimiento del lineamiento establecido en el numeral 10.2 *"Acciones Correctivas y no conformidades"*, del MSPI.

De otra parte, teniendo en cuenta que, (i) las actividades propuestas en el marco del Plan de Mejoramiento PM-23-AI2023, tenían como fecha máxima de cumplimiento el mes de diciembre de 2023, (ii) según se evidenció en las comunicaciones remitidas por la OPGI no se habían recibido hasta el mes de julio de 2025 los soportes de implementación y/o cumplimiento y que (iiii) a la fecha 24 de septiembre de 2025, no se recibieron los soportes de cumplimiento de las actividades propuestas en el marco del Plan de Mejoramiento PM-23-AI2023 acorde a la solicitud realizada por la Oficina de Control Interno el día 11 de septiembre, como parte de la verificación realizada en el desarrollo de la presente auditoría.

Así las cosas, se identifica que el plan de mejoramiento *PM-23-AI2023-07* no fue eficaz, toda vez que no se cuenta con los soportes de cumplimiento y por tanto dichas acciones tampoco fueron efectivas para mitigar las causas que dieron origen al hallazgo.

A partir de lo anterior se registran los resultados de la evaluación de efectividad en el Anexo 1 del presente informe identificado como: "Anexo 1 E-ME-F-11 FORMATO PLAN DE MEJORA PM-23-AI2023-07.pdf"

Criterio(s):

Resolución 02277 de 2021 *""Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia"*

"ARTÍCULO 1*. Actualización del Anexo 1 de la Resolución 500 de 2021. Actualícese el Anexo 1 de la Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", el cual será publicado en la sede electrónica del Ministerio de Tecnologías de la Información y las Comunicaciones, a más tardar quince (15) días siguientes a la expedición de la presente resolución".*

Anexo 1 de la Resolución 02277 - Modelo de Seguridad y Privacidad de la Información:

10.2. Acciones Correctivas y no conformidades

Lineamiento: "Ante una no conformidad, la entidad debe corregirla, mitigar sus efectos y evaluar acciones para evitar su repetición.":

***Norma ISO 27001 numeral* 10.2 "NO CONFORMIDADES Y ACCIONES CORRECTIVAS"**

"(...) Cuando se presenta una no conformidad, la organización debe:
a. Reaccionar ante la no conformidad, y según aplique:
1. Tomar acciones para controlarla y corregirla;
2. Enfrentar las consecuencias; de riesgos y estado del plan de tratamiento de riesgos;(...)

(...) c. Implementar cualquier acción requerida;
d. Revisar la eficacia de cualquier acción tomada."

Posible(s) causa(s) identificada(s) por la Oficina de Control Interno

- Desconocimiento de lineamientos dados por el Documento Maestro del MSPI.
- Posible falta de conocimiento de lineamientos para la formulación/reformulación de planes de mejoramiento
- Posible falta de aprobación de documentos y lineamientos internos de seguridad de la Información requeridos por el MSPI y documentación de acciones de mejora.
- Debilidades en la implementación de acciones de mejora por parte de la primera línea de defensa.
- Posibles debilidades en la evaluación de eficacia de acciones de mejora por parte de la segunda línea defensa.

Posible(s) Consecuencias o efectos (s) identificado(s) por la Oficina de Control Interno

- Afectación a la toma de Decisiones por parte de la Dirección en lo relacionado con la gestión de riesgos, e implementación de controles de seguridad de la información del Ministerio de Minas y Energía asociados al plan de recuperación de desastres y el análisis de impacto en el negocio (BIA).
- Posible afectación a la disponibilidad, integridad y confidencialidad de activos de información críticos de la Entidad relacionados con el plan de recuperación de desastres y el análisis de impacto en el negocio (BIA).
- Posibles debilidades en la adopción de acciones de mejora a fin de asegurar e cumplimiento de condiciones de seguridad de la Información al interior de la Entidad.

Recomendación(nes) específica(s):

- Evaluar la pertinencia de definir y documentar los lineamientos para la revisión de eficacia de acciones y presentación de resultados dentro de la "Revisión por la

Dirección" ante el Comité Institucional de Gestión y Desempeño, periódicamente (anual, semestral, etc).

- Adelantar la reformulación de acciones relacionadas con el plan de mejoramiento "*PM-23-AI2023-07*" incluyendo actividades relacionadas con el seguimiento y verificación de cronogramas de cumplimiento de acciones de mejora por parte del Grupo TIC's.
- Evaluar la pertinencia de definir controles preventivos y rutinas de seguimiento al cumplimiento de planes de mejoramiento derivados de ejercicios de evaluación interna y externa a fin de asegurar la adecuada gestión de las mejoras requeridas en la gestión del proceso de Gestión de Tecnologías de Información y las Comunicaciones, así como del Sistema de gestión de Seguridad de la Información.
- Evaluar la pertinencia de articular los elementos de implementación del Sistema de Gestión de Seguridad de la Información con el Sistema Integrado de Gestión SIG.

Notas finales:

- La naturaleza de la labor de auditoría interna ejecutada por la Oficina de Control Interno, al estar supeditada al cumplimiento del Programa Anual de Auditoría, se encuentra limitada por restricciones de tiempo y alcance, razón por la que procedimientos más detallados podrían develar asuntos no abordados en la ejecución de esta actividad.
- La evidencia recopilada para propósitos de la evaluación efectuada versa en información suministrada por (dependencias proveedoras de información durante la auditoría interna), a través de solicitudes y consultas realizadas por la Oficina de Control Interno. Nuestro alcance no pretende corroborar la precisión de la información y su origen.
- Es necesario precisar que, las "Recomendaciones" propuestas en ningún caso son de obligatoria ejecución por parte de la Entidad, más se incentiva su consideración para los planes de mejoramiento a que haya lugar.
- La respuesta ante las situaciones observadas por la Oficina de Control Interno es discrecional de la Administración de la Entidad.

YANETH RODRIGUEZ BUSTOS
JEFA OFICINA DE CONTROL INTERNO (E)

Elaboró: Rigoberto Andres Vaca Pardo - Contratista