Acceso: Reservado ( ), Público (X), Clasificada().

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

Elaboró:

Secretaría General - Grupo de Tecnologías de la Información y las Comunicaciones (GTIC)

Jairo Andrés Grajales Salinas
Leidy Paola Galindo Acevedo
Andrés Camilo Molano Mendieta

Entidad:

Ministerio de Minas y Energía

Bogotá, 16 de Julio de 2025

Ministerio de Minas y Energía

Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Energía

Contenido

1. PROCESO 3

2. RESPONSABLE DEL PROCESO 3

3. DESCRIPCIÓN INFORME 3

4. PLAN OPERACIONAL DE SEGURIDAD DE LA INFORMACIÓN 4

4.1 GESTIÓN DE ACTIVOS DE INFORMACIÓN 4

4.2 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 7

4.3 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 12

Riesgo R5: “Implementación de código seguro” 12

Riesgo R11 Habilitar y configurar el módulo de auditoría de los SI (aplicaciones, Web Services, Apps, entre otros) acorde con capacidades y necesidades. 17

Riesgo R14 Realizar las tareas y actividades de backup, respaldo ydisposición acorde con plan de programación y/o solicitudes puntuales. 23

R23: Procedimiento Gestión de Continuidad y Recuperación de los Servicios de Informática y Comunicaciones. Ausencia de DRP actualizado. 27

4.4 GESTIÓN DE POLÍTICAS Y PROCEDIMIENTOS 29

4.5 GESTIÓN DE RECURSOS DE SEGURIDAD 32

5. SEGUIMIENTO PLAN DE ASEGURAMIENTO Y EVALUACIÓN DE LA IMPLEMENTACIÓN Y MANTENIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN 35

5.1 GESTIÓN DE INDICADORES 35

5.2 GESTIÓN DE VULNERABILIDADES. 37

5.3 PLAN DE AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN 42

6. CAPACITACIÓN Y SENSIBILIZACIÓN 43

Ministerio de Minas y Energía

Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia

Conmutador: +57 (601) 220 0300

1. PROCESO

Gestión tecnológica.

2. RESPONSABLE DEL PROCESO

Grupo de Tecnologías de la Información y las Comunicaciones
Ing. Jairo Andrés Grajales Salinas
Coordinador Grupo TIC
Email: aaayure@minenergia.gov.co
Teléfono: (+57) 6012200300 Ext. 2408

3. DESCRIPCIÓN INFORME

El Plan de Seguridad y Privacidad de la Información, es el resultado de un diagnóstico y planeación para el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), conforme la evolución y actualización de las tecnologías de la información y comunicaciones (TIC). También se mejoraron las políticas, procedimientos y guías que permitieron al Ministerio de Minas y Energía MINENERGÍA, cumplir los requerimientos del Modelo de Seguridad y Privacidad de la información (MSPI) buscando la mejora continua.

El Plan de Seguridad y Privacidad de la Información, contiene los lineamientos del Modelo de Seguridad y Privacidad de la MSPI versión 3.0.2 definido por Ministerio de Tecnologías de la Información y Comunicaciones en adelante MINTIC, el cual orienta a las entidades del estado colombiano en la preservación de la confidencialidad, integridad y disponibilidad de la información, además permite fijar los criterios para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información.

Para la elaboración de este documento, se toma como referencia además de los lineamientos de MINTIC en el MSPI y sus correspondientes guías de apoyo, las normas ISO/IEC 27001:2022, ISO/IEC 22301:2019 e ISO/IEC 31000:2018.

4. PLAN OPERACIONAL DE SEGURIDAD DE LA INFORMACIÓN

4.1 GESTIÓN DE ACTIVOS DE INFORMACIÓN

En el segundo trimestre de 2025 se completó la implementación del instrumento único de gestión de activos de información, consolidando en una primera fase los catálogos de licenciamiento, sistemas de información e infraestructura elaborados junto al equipo de Arquitectura Empresarial, de esta manera, se puede continuar con la capacitación a los lideres SIG de la entidad para el diligenciamiento adecuado y paralelo a esto continuar con la estructuración de los BCP y BIA correspondientes.

No obstante, con la entrada en vigor del nuevo Modelo de Seguridad y Privacidad de la Información (MSPI), se identificó la necesidad de incorporar un módulo específico para la identificación de infraestructura crítica cibernética. Por ello, el instrumento está en proceso de revisión y ajuste durante el tercer trimestre, de modo que, una vez actualizado, permita un solo ejercicio integrado de valoración de activos y continuidad operacional acorde con los lineamientos del MSPI.

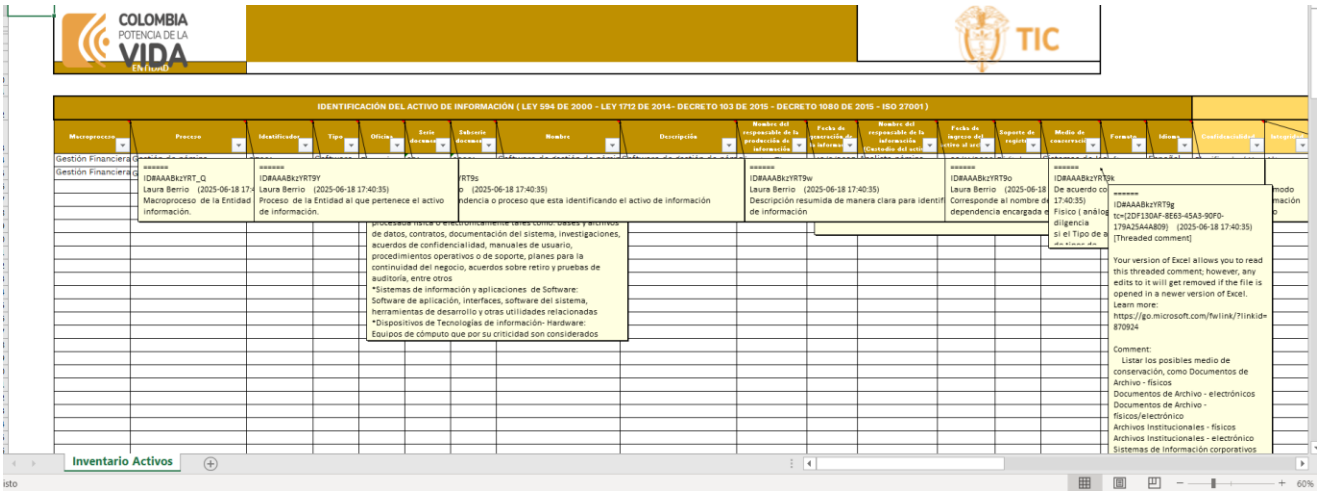


Imagen [11]. Revisión y comparación con el nuevo modelo de MINTIC 2025 frente al instrumento de clasificación de activos de información.

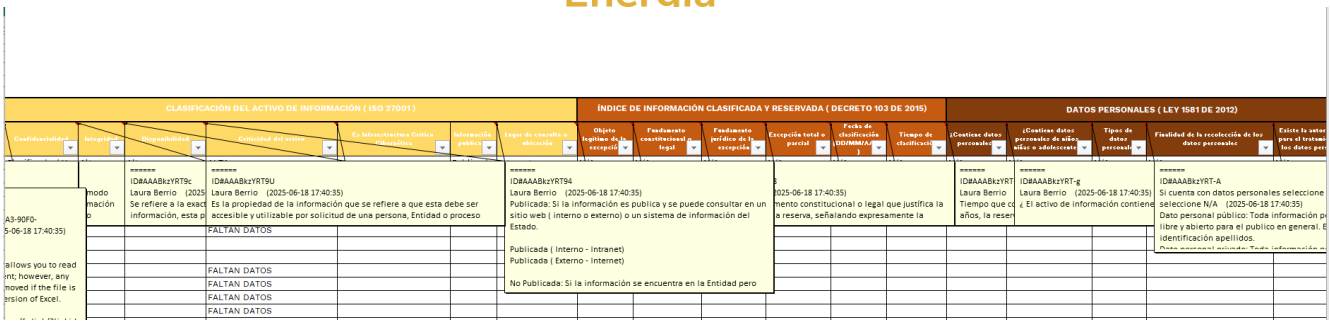


Imagen [2]. Comparación frente al índice información clasificada y reservada .

Además de esto, ha venido adelantando un proyecto de inversión enfocado en el fortalecimiento estructural del Modelo de Seguridad y Privacidad de la Información (MSPI). Este proyecto, actualmente en etapa contractual, contempla la revisión integral de los activos de información institucionales como eje estratégico para el cierre de brechas normativas, técnicas y operativas identificadas en el diagnóstico inicial. La gestión de estos activos se concibe bajo un enfoque holístico que incluye activos digitales, físicos e intangibles, alineados con los lineamientos del Decreto 338 de 2022, la Resolución 40646 de 2023 y normas internacionales como ISO/IEC 27001:2022 e ISO/IEC 22301:2019.

Uno de los componentes fundamentales del proyecto es la actualización y depuración del inventario de activos de información, garantizando su registro en una herramienta GRC (Gobernanza, Riesgo y Cumplimiento) que será implementada por el contratista adjudicatario. Esta herramienta permitirá identificar, clasificar, valorar y vincular cada activo con sus respectivos procesos, riesgos, controles y responsables, asegurando su trazabilidad y facilitando el análisis de criticidad. Se dará prioridad a los activos relacionados con infraestructuras críticas del sector minero-energético, los cuales serán categorizados según su nivel de sensibilidad, impacto potencial y requerimientos de protección, en cumplimiento con lo establecido por el Decreto 338 y la Política Nacional de Seguridad y Confianza Digital.

El enfoque adoptado no se limita al inventario, sino que abarca una estrategia más amplia que incluye la revisión y actualización de políticas, roles y procedimientos, así como la implementación de mecanismos tecnológicos como plataformas GRC y soluciones de desarrollo seguro (Secure SDLC). Estas acciones permitirán reforzar el ciclo PHVA del MSPI, establecer controles efectivos desde el diseño (privacy by design y security by design) e incorporar capacidades avanzadas de ciberinteligencia y Zero Trust. De manera complementaria, se desarrollarán campañas de sensibilización, formación técnica y auditorías internas, con el fin de asegurar la sostenibilidad del modelo y su integración con otros sistemas de gestión como el MIPG, el Sistema de Gestión de Calidad (SGC) y la Arquitectura Empresarial institucional.

Teniendo en cuenta lo anterior y analizando este nuevo contexto de integración para establecer un único instrumento que sirva a todas áreas del ministerio se debe actualizar el cronograma ya planteado en el "plan de seguridad y privacidad de la información 2025", con base a esto se tiene la siguiente tabla:

Tabla 1.
Actualización cronograma de actividades- Matriz de activos de información

Actividad	Responsable	Fecha de Inicio	Fecha de Finalización	Descripción
Capacitación sobre la matriz de activos	Oficial de Seguridad o quien haga sus veces	Segunda semana – Agosto 2025	Cuarta semana – Agosto 2025	Capacitar a los responsables en el uso de la matriz y en los principios básicos de activos de información.
Llenado inicial de la matriz de activos	Lideres SIG	Primera semana - Septiembre 2025	Tercera semana - Septiembre 2025	Identificar y clasificar activos de información según los procesos de cada área
Revisión primaria de información enviada por las dependencias	Oficial de Seguridad o quien haga sus veces – Gestión documetal	Tercera semana - Octubre 2025	Cuarta semana – Octubre 2025	Revisar documentación enviada por las dependencias (responsables) , unificar información y establecer retroalimentación y mejora continua.
Ajustes y envío de retroalimentación a dependencias	Oficial de Seguridad o quien haga sus veces	Cuarta semana - Octubre 2025	Primera Semana - Octubre 2025	En caso de presentarse información faltante o incompleta generar retroalimentación.
Entrega de información ajustada	Responsables de cada dependencia	Segunda Semana - Noviembre 2025	Cuarta semana – Noviembre 2025	Información debidamente ajustada y completada.
Validación y priorización de activos críticos	Oficial de Seguridad o quien haga sus veces	Primera semana - Diciembre 2025	Segunda semana - Diciembre 2025	Revisar, validar y priorizar los activos críticos según el impacto al negocio y continuidad al mismo.

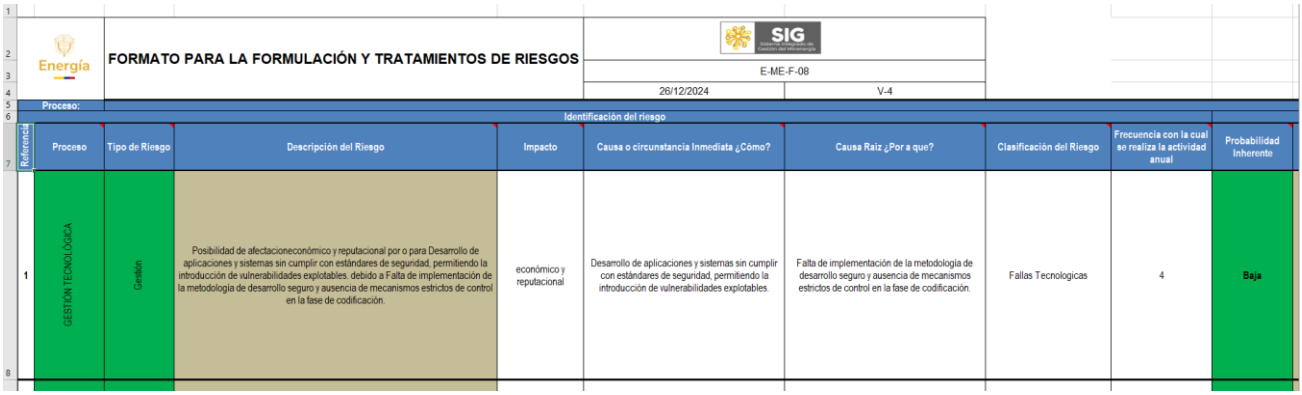
Integración con el SGSI	Oficina de planeación y gestión territorial	Diciembre 2025	Diciembre 2025	Incorporar los activos priorizados en el SGSI y actualizar los controles.

Fuente grupo TICS

4.2 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de riesgos de seguridad de la información desempeña un papel crucial para el Ministerio de Minas y Energía al enfrentar los desafíos y oportunidades en un entorno digital dinámico y cada vez más complejo. Al identificar, evaluar y mitigar los riesgos de seguridad de la información, el Ministerio no solo protege los activos críticos de datos y sistemas, sino que también salvaguarda la confianza pública y fortalece su capacidad para cumplir con las obligaciones regulatorias. Además, una gestión efectiva de riesgos proporciona una base sólida para la toma de decisiones informadas, promoviendo la continuidad operativa y minimizando el impacto de posibles incidentes de seguridad.

A partir de ello y siguiendo la hoja de ruta de gestión de seguridad de la información se definen los siguientes riesgos para esta vigencia 2025 teniendo en cuenta el actual contexto de la entidad y sus fines misionales y estratégicos de gestión tecnológica :



Energía	FORMATO PARA LA FORMULACIÓN Y TRATAMIENTOS DE RIESGOS	SIG	
		E-ME-F-08	
		26/12/2024	V-4

Proceso:

Identificación del riesgo									
Referencia	Proceso	Tipo de Riesgo	Descripción del Riesgo	Impacto	Causa o circunstancia Inmediata ¿Cómo?	Causa Raiz ¿Por a que?	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad anual	Probabilidad Inherente
1	GESTIÓN TECNOLÓGICA	Gestión	Posibilidad de afectacioneconómico y reputacional por o para Desarrollo de aplicaciones y sistemas sin cumplir con estándares de seguridad, permitiendo la introducción de vulnerabilidades explotables. debido a Falta de implementación de la metodología de desarrollo seguro y ausencia de mecanismos estrictos de control en la fase de codificación.	económico y reputacional	Desarrollo de aplicaciones y sistemas sin cumplir con estándares de seguridad, permitiendo la introducción de vulnerabilidades explotables.	Falta de implementación de la metodología de desarrollo seguro y ausencia de mecanismos estrictos de control en la fase de codificación.	Fallas Tecnologicas	4	Baja

Imagen [3]. Riesgo 1 (R5) , causa inmediata y causa raíz y descripción del riesgo.

Análisis del riesgo inherente						Evaluación del riesgo - Valoración de los controles TODOS LOS PROCESOS			
%	Impacto	Observación de criterio	Impacto Inherente	%	Zona de Riesgo Inherente	No. Control	Descripción del Control	Cargo del responsable del control	Acción que realiza
40%	Entre 50 y 100 SMLMV	Entre 50 y 100 SMLMV	Moderado	60%	Moderado	1	El funcionario del grupo TICs designado para la seguridad y privacidad aplica el checklist de seguridad definido en la metodologia de desarrollo del ministerio, basado en estándares internacionales como OWASP y PCI DSS, adicionalmente, programa auditorias trimestrales en los sistemas de información para evaluar la correcta implementación de los lineamientos de código seguro, si encuentra inconsistencias en la auditoria solicita ajustes; adicionalmente, realiza pruebas de penetración (pentesting) y análisis de vulnerabilidades en entornos controlados, asegurando la detección y mitigación de riesgos antes de la puesta en producción.	Funcionario	1. Aplicar el checklist de seguridad definido en la metodologia de desarrollo del ministerio, basado en estándares internacionales como OWASP y PCI DSS. 2. Programar auditorias trimestrales en los sistemas de información para evaluar la correcta implementación de los lineamientos de código seguro. 3. Realizar pruebas de penetración (pentesting) y análisis de vulnerabilidades en entornos controlados, asegurando la detección y mitigación de riesgos antes de la puesta en producción.

Imagen [4].Mapa de calor y zona de riesgo determinada, control y acciones a realizar (R5).

2	GESTIÓN TECNOLÓGICA	Gestión	Posibilidad de afectacioneconómico y reputacional por o para Ausencia de supervisión continua de registros de actividad en los sistemas de información, permitiendo que incidentes de seguridad pasen desapercibidos. debido a Falta de un procedimiento estandarizado para la gestión y análisis de logs de seguridad, junto con la ausencia de herramientas automatizadas de monitoreo y alerta.	económico y reputacional	Ausencia de supervisión continua de registros de actividad en los sistemas de información, permitiendo que incidentes de seguridad pasen desapercibidos.	Falta de un procedimiento estandarizado para la gestión y análisis de logs de seguridad, junto con la ausencia de herramientas automatizadas de monitoreo y alerta.	Ejecucion y Administracion de procesos	4	Baja

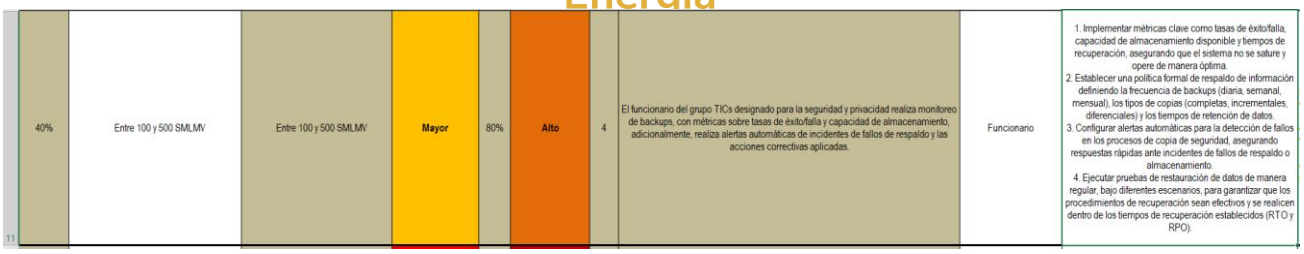
Imagen [5]. Riesgo 2 (R11) , causa inmediata y causa raíz y descripción del riesgo.

40%	Entre 100 y 500 SMLMV	Entre 100 y 500 SMLMV	Mayor	80%	Alto	2	El funcionario del grupo TICs designado para la seguridad y privacidad revisa que los sistemas de información críticos del Ministerio tengan módulos de auditoria, adicionalmente, configura alertas automáticas para detectar comportamientos sospechosos en aplicaciones, bases de datos y redes, asegurando una respuesta oportuna ante posibles incidentes.	Funcionario	1.Desarrollar y documentar un procedimiento estandarizado para la implementación de módulos de auditoria en todos los sistemas de información críticos del Ministerio. 2.Implementar soluciones de monitoreo centralizado que permitan la recolección, análisis y correlación de eventos de seguridad en tiempo real. 3.Configurar alertas automáticas para detectar comportamientos sospechosos en aplicaciones, bases de datos y redes, asegurando una respuesta oportuna ante posibles incidentes.

Imagen [6].Mapa de calor y zona de riesgo determinada, control y acciones a realizar (R11).

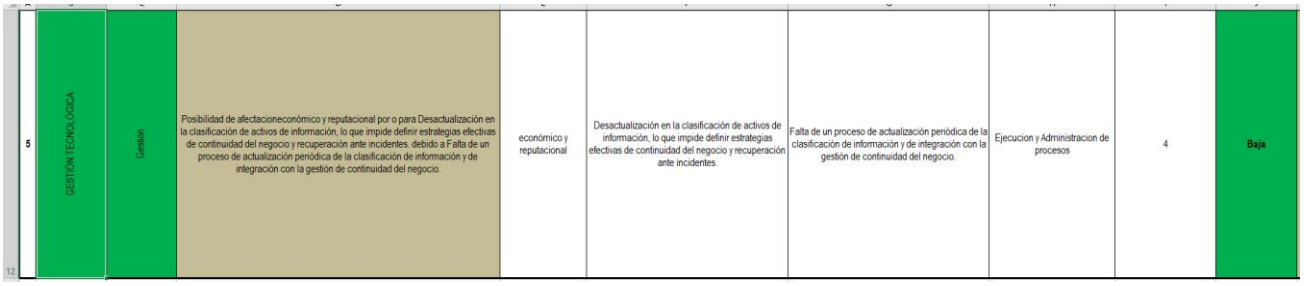
4	GESTIÓN TECNOLÓGICA	Gestión	Posibilidad de afectacioneconómico y reputacional por o para Pérdida de información crítica debido a fallos en los procesos de respaldo, almacenamiento y recuperación de datos, afectando la continuidad operativa del ministerio. debido a Ausencia de un proceso estructurado de respaldo de información y monitoreo de la efectividad de los backups.	económico y reputacional	Pérdida de información crítica debido a fallos en los procesos de respaldo, almacenamiento y recuperación de datos, afectando la continuidad operativa del ministerio.	Ausencia de un proceso estructurado de respaldo de información y monitoreo de la efectividad de los backups.	Fallas Tecnologicas	4	Baja

Imagen [7]. Riesgo 3 (R14) , causa inmediata y causa raíz y descripción del riesgo.



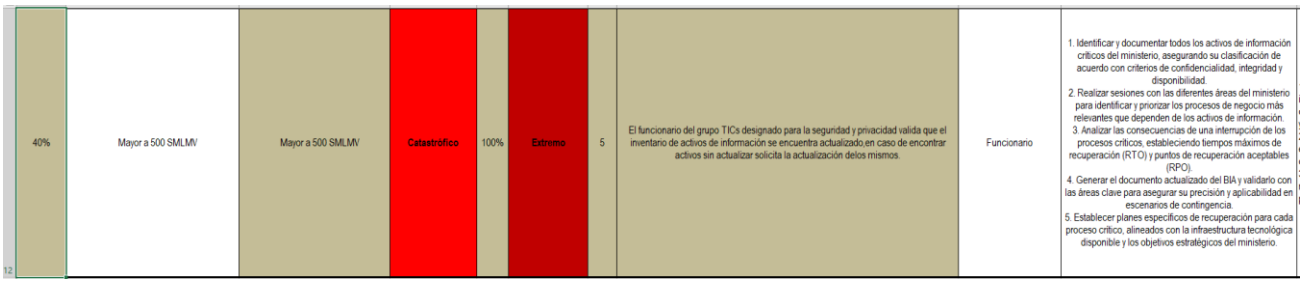
11	40%	Entre 100 y 500 SMLMV	Entre 100 y 500 SMLMV	Mayor	80%	Alto	4	El funcionario del grupo TICs designado para la seguridad y privacidad realiza monitoreo de backups, con métricas sobre tasas de éxito/falla y capacidad de almacenamiento, adicionalmente, realiza alertas automáticas de incidentes de fallos de respaldo y las acciones correctivas aplicadas.	Funcionario	1. Implementar métricas clave como tasas de éxito/falla, capacidad de almacenamiento disponible y tiempos de recuperación, asegurando que el sistema no se sature y opere de manera óptima. 2. Establecer una política formal de respaldo de información definiendo la frecuencia de backups (diaria, semanal, mensual), los tipos de copias (completas, incrementales, diferenciales) y los tiempos de retención de datos. 3. Configurar alertas automáticas para la detección de fallos en los procesos de copia de seguridad, asegurando respuestas rápidas ante incidentes de fallos de respaldo o almacenamiento. 4. Ejecutar pruebas de restauración de datos de manera regular, bajo diferentes escenarios, para garantizar que los procedimientos de recuperación sean efectivos y se realicen dentro de los tiempos de recuperación establecidos (RTO y RPO).

Imagen [8].Mapa de calor y zona de riesgo determinada, control y acciones a realizar (R14).



12	5	GESTIÓN TECNOLÓGICA	Gestion	Posibilidad de afectacioneconómico y reputacional por o para Desactualización en la clasificación de activos de información, lo que impide definir estrategias efectivas de continuidad del negocio y recuperación ante incidentes. debido a Falta de un proceso de actualización periódica de la clasificación de información y de integración con la gestión de continuidad del negocio.	económico y reputacional	Desactualización en la clasificación de activos de información, lo que impide definir estrategias efectivas de continuidad del negocio y recuperación ante incidentes.	Falta de un proceso de actualización periódica de la clasificación de información y de integración con la gestión de continuidad del negocio.	Ejecucion y Administracion de procesos	4	Baja

Imagen [9]. Riesgo 4 (R21) , causa inmediata y causa raíz y descripción del riesgo.



12	40%	Mayor a 500 SMLMV	Mayor a 500 SMLMV	Catastrófico	100%	Extremo	5	El funcionario del grupo TICs designado para la seguridad y privacidad valida que el inventario de activos de información se encuentra actualizado,en caso de encontrar activos sin actualizar solicita la actualización delos mismos.	Funcionario	1. Identificar y documentar todos los activos de información críticos del ministerio, asegurando su clasificación de acuerdo con criterios de confidencialidad, integridad y disponibilidad. 2. Realizar sesiones con las diferentes áreas del ministerio para identificar y priorizar los procesos de negocio más relevantes que dependen de los activos de información. 3. Analizar las consecuencias de una interrupción de los procesos críticos, estableciendo tiempos máximos de recuperación (RTO) y puntos de recuperación aceptables (RPO). 4. Generar el documento actualizado del BIA y validarlo con las áreas clave para asegurar su precisión y aplicabilidad en escenarios de contingencia. 5. Establecer planes específicos de recuperación para cada proceso crítico, alineados con la infraestructura tecnológica disponible y los objetivos estratégicos del ministerio.

Imagen [10].Mapa de calor y zona de riesgo determinada, control y acciones a realizar (R21).

Teniendo en cuenta lo anterior se deja a continuación un tabla donde se especifica el riesgo y sus acciones concretas a realizar para mitigar el mismo, para mayor información del cronograma de cumplimiento revisar el “plan de tratamiento de riesgos de seguridad de la información” :

Tabla 2

Tabla de riesgos para vigencia 2025

No. Riesgo	NOMBRE DEL RIESGO
R5	Implementación de código seguro **Actividades necesarias:** 1. Aplicar el checklist de seguridad definido en la metodología de desarrollo del Ministerio, basado en estándares internacionales como OWASP y PCI DSS. 2. Programar auditorías trimestrales en los sistemas de información para evaluar la correcta implementación de los lineamientos de código seguro. 3. Realizar pruebas de penetración (pentesting) y análisis de vulnerabilidades en entornos controlados, asegurando la detección y mitigación de riesgos antes de la puesta en producción.
R11	Falta de monitoreo a Logs de seguridad y registro **Actividades necesarias:** 1. Desarrollar y documentar un procedimiento estandarizado para la implementación de módulos de auditoría en todos los sistemas de información críticos del Ministerio. 2. Implementar soluciones de monitoreo centralizado que permitan la recolección, análisis y correlación de eventos de seguridad en tiempo real. 3. Configurar alertas automáticas para detectar comportamientos sospechosos en aplicaciones, bases de datos y redes, asegurando una respuesta oportuna ante posibles incidentes.
R14	Gestión de Backups **Actividades necesarias:** 1. Implementar métricas clave como tasas de éxito/falla, capacidad de almacenamiento disponible y tiempos de recuperación, asegurando que el sistema no se sature y opere de manera óptima, esto determinará si se continua con esta herramienta de respaldo o si se debe reemplazar por otra que cumpla los estándares necesarios. 2. Establecer una política formal de respaldo de información definiendo la frecuencia de backups (diaria, semanal, mensual), los tipos de copias (completas, incrementales, diferenciales) y los tiempos de retención de datos.

	3. Establecer alertas automáticas para la detección de fallos en los procesos de copia de seguridad, asegurando respuestas rápidas ante incidentes de fallos de respaldo o almacenamiento. 4. Ejecutar pruebas de restauración de datos de manera regular, bajo diferentes escenarios, para garantizar que los procedimientos de recuperación sean efectivos y se realicen dentro de los tiempos de recuperación establecidos (RTO y RPO).
R21	Falencias en la clasificación de información – sin actualización desde 2021 No se tiene por ende BIA y BCP actualizados. **Actividades necesarias:** 1. Identificar y documentar todos los activos de información críticos del Ministerio, asegurando su clasificación de acuerdo con criterios de confidencialidad, integridad y disponibilidad. 2. Realizar sesiones con las diferentes áreas del Ministerio para identificar y priorizar los procesos de negocio más relevantes que dependen de los activos de información. 3. Analizar las consecuencias de una interrupción de los procesos críticos, estableciendo tiempos máximos de recuperación (RTO) y puntos de recuperación aceptables (RPO). 4. Generar el documento actualizado del BIA y validarlo con las áreas clave para asegurar su precisión y aplicabilidad en escenarios de contingencia. 5. Establecer planes específicos de recuperación para cada proceso crítico, alineados con la infraestructura tecnológica disponible y los objetivos estratégicos del Ministerio.

4.3 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Atendiendo las indicaciones y recomendaciones de la Oficina de Planeación y Gestión Internacional, en el sentido que, para la presente vigencia este Plan, se adaptara y adoptara la misma metodología de trabajo dispuesta desde la "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6", expedida por el DAFP en noviembre de 2022, para lo cual los riesgos descritos tanto en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, como los riesgos de la gestión TIC, tendrán seguimiento y control trimestral durante la vigencia 2025.

Riesgo R5: "Implementación de código seguro"

1. **Realizar los ajustes y cambios en la metodología de desarrollo en donde se han incorporado los temas de código seguro, Programar auditorías trimestrales en los sistemas de información para evaluar la correcta implementación de los lineamientos de código seguro.**

2. **Realizar pruebas de penetración (pentesting) y análisis de vulnerabilidades en entornos controlados, asegurando la detección y mitigación de riesgos antes de la puesta en producción.**

Acorde a los lineamientos del MSPI y la normatividad de código seguro que se debe implementar en desarrollo de software, se finaliza en el segundo trimestre del 2024 el documento de "Metodología y Arquitectura de Referencia para el Desarrollo de Sistemas de Información y Nuevas Aplicaciones del Ministerio De Minas y Energía" anexando los numerales 8 y 9. En el primero, se establece el proceso de construcción seguro de software donde se determina lo siguiente:

1. Análisis de requerimientos (según necesidad y criticidad de la información).
2. Desarrollo – requerimientos y procesos con mínimos de seguridad
3. Pruebas – Entornos de Sandbox para análisis de vulnerabilidades y riesgos.

4. Despliegue o puesta en marcha – Seguimiento de posibles vulnerabilidades deataques de día cero.

5. Capacitación y concientización de las buenas prácticas de desarrollo.

A través de dicho proceso se estableció un "check list" de preguntas fundamentales para que el desarrollador/a al momento de evaluar el requerimiento y finalizar su responsabilidad pueda determinar si está cumpliendo con la metodología establecida,dicho documento se centra en los siguientes conceptos:

Tabla 5. Conceptos de checklist de código seguro.

N°	CONCEPTO
1	Patrones de Diseño Seguros
2	Anti-patrones a evitar
3	Arquitecturas Seguras
4	Prácticas de Desarrollo Seguro
5	Principio de Privilegio Mínimo
6	Ciclo de Vida de Desarrollo Seguro (SDLC)
7	Revisiones de Código y Pruebas
8	Seguridad en la Infraestructura

En el segmento número 9 se establecen según guías y normatividad internacional *"OWASP Top 10 y PCI DSS" los* riesgos más significativos que se tienen durante el desarrollo de software y sus recomendaciones para lograr los mejores resultados.

El informe correspondiente a Junio de 2025 presenta un balance técnico detallado de las actividades desarrolladas por el equipo de software, con especial atención en la mitigación de riesgos asociados a corrupción y a la introducción de vulnerabilidades en el código. Se evidencia un control riguroso sobre la documentación, trazabilidad, cumplimiento normativo, cesión de derechos patrimoniales de software y verificación de licencias en sistemas nuevos desarrollados en Open Source de la siguiente manera :

"Con el propósito de modernizar la arquitectura tecnológica del Ministerio de Minas y Energía (MME), se ha llevado a cabo la adopción de herramientas de software libre (Open Source) que responden a necesidades de desarrollo interno, gestión de proyectos, soporte técnico y automatización de servicios digitales. Esta estrategia se enmarca en los principios de eficiencia,

sostenibilidad, autonomía tecnológica y buenas prácticas de gobierno digital"

Herramientas Implementadas y Resultados

Taiga – Plataforma de gestión de proyectos ágiles

Funcionalidades destacadas:

- Planificación de sprints y tareas mediante tableros Kanban.

- Creación de *epics*, *user stories* y tareas técnicas asociadas.
- Seguimiento de avance por hitos y métricas de productividad del equipo.
- Integración con GitLab para vincular código a tareas del proyecto.

Resultado:

- Se logró una mejor coordinación entre los equipos de desarrollo, análisis y arquitectura.
- Se redujeron los tiempos de planificación y priorización de requerimientos.
- Aumentó la transparencia del avance de proyectos estratégicos para la entidad.
- Se estableció una cultura ágil y colaborativa dentro de la Subdirección de Tecnología.

GitLab – Repositorio de código fuente y automatización DevOps

Funcionalidades destacadas:

- Gestión de múltiples repositorios con permisos por proyecto.
- Control de versiones mediante Git, gestión de *branches*, *merge requests* y revisión de código.
- Automatización de pruebas y despliegues (CI/CD).
- Webhooks y *runners* para integración con servicios como Taiga y Nexus.

Resultado:

- Se garantiza la trazabilidad del ciclo de vida del desarrollo, desde el requerimiento hasta el despliegue.
- Reducción de errores humanos mediante automatización de pruebas y despliegue continuo.
- Refuerzo de la gobernanza del código con *revisiones cruzadas*, estándares de codificación y trazabilidad de cambios.

GLPI – Gestión de incidentes y mesa de ayuda institucional

Funcionalidades destacadas:

- Registro de tickets para soporte técnico, solicitudes de acceso, fallas de hardware/software, entre otros.
- Clasificación automática por tipo de solicitud y dependencia responsable.
- Base de conocimientos para autoayuda y documentación de soluciones frecuentes.
- Panel de métricas por analista, por tipo de incidente y tiempos de atención.

Resultado:

- Mayor eficiencia en la atención a usuarios internos del MME.

- Reducción en los tiempos promedio de resolución de incidentes.
- Seguimiento detallado de la demanda de soporte técnico, útil para toma de decisiones.
- Generación de reportes mensuales para identificar cuellos de botella y áreas de mejora.

Nexus Repository – Almacenamiento local de imágenes docker

Funcionalidades destacadas:

- Registro privado para imágenes Docker utilizadas por los sistemas de la entidad.
- Control de versiones de contenedores desplegados en ambientes de desarrollo, pruebas y producción.
- Aseguramiento de disponibilidad en entornos con restricciones de conectividad.
- Integración directa con los *pipelines* de GitLab para automatizar la publicación de imágenes.

Resultado:

- Se asegura un entorno confiable, seguro y auditable para el despliegue de microservicios.
- Mayor independencia respecto a servicios de terceros, alineado con la política de soberanía digital.
- Mejora en la velocidad de despliegue en entornos controlados (on-premises).
- Permite mantener un control riguroso sobre el ciclo de vida de las imágenes y sus vulnerabilidades.

Plataformas de desarrollo implementadas

Laravel – Desarrollo del sistema de asistencias y carnet virtual

Casos de uso:

- Registro, seguimiento y validación de asistencias del personal.
- Generación dinámica del carnet digital de identificación institucional.
- Control de permisos, roles, notificaciones y validaciones en línea.

Ventajas:

- Rapidez en el desarrollo de interfaces limpias y seguras.
- Facilidad de integración con bases de datos relacionales y APIs REST.
- Comunidad activa y soporte continuo.

Resultado:

- Sistema de asistencias implementado en producción con altos niveles de satisfacción.
- Validación de identidad institucional desde dispositivos móviles mediante código QR.
- Reducción de procesos manuales y dependencia de formatos impresos.

3.2 Python + Vue.js – Desarrollo de la Ventanilla Única de Trámites

Arquitectura:

- Backend en Python (FastAPI), con procesamiento asincrónico y alto rendimiento.
- Frontend en Vue.js, adaptable a múltiples dispositivos (responsive).
- Autenticación integrada con servicios institucionales.

Casos de uso:

- Unificación de trámites de la entidad en una sola interfaz.
- Seguimiento en tiempo real del estado del trámite por parte del ciudadano.
- Interacción con otras plataformas públicas vía interoperabilidad.

Resultado:

- Modernización de la experiencia ciudadana al eliminar procesos presenciales.
- Estandarización y trazabilidad de los trámites internos.
- Reducción significativa de tiempos de atención y validación por parte de las áreas responsables.

En el marco de este plan de tratamiento, se implementaron buenas prácticas como el uso de repositorios oficiales (GitLab), metodologías ágiles apoyadas en herramientas como Taiga, y la revisión conjunta con proveedores en procesos contractuales para asegurar la entrega conforme a los requerimientos. También se promovió el uso de software libre (GLPI, Bitwarden, Taiga) evaluando sus implicaciones de seguridad e interoperabilidad. A través de sesiones técnicas, validaciones normativas y aseguramiento de la calidad, se busca garantizar que los sistemas de información desarrollados e implementados respondan a criterios de integridad, confidencialidad y disponibilidad, alineados con la estrategia institucional de gestión de riesgos de seguridad de la información.

Con base a lo anterior se ejecutan actividades de escaneo de vulnerabilidades, donde se evidencian algunas brechas de seguridad de carácter alto y medio , en este listado se encuentran 3 aplicativos, los cuales están en proceso de acciones a tomar para la mitigación de dichos requerimientos y que no generan brechas de seguridad que acarreen en incidente de seguridad futuros.

Para más información en relación con la mitigación de este riesgo (R5) de la metodología que tiene y actualiza el MINENERGÍA, se sugiere remitirse al líder del equipo de Desarrollo del Grupo TICS y en todo lo concerniente al tema de vulnerabilidades al oficial de seguridad de la información o quien haga sus veces.

Riesgo R11 Habilitar y configurar el módulo de auditoría de los SI (aplicaciones, Web Services, Apps, entre otros) acorde con capacidades y necesidades.

Actividad 2: Implementar soluciones de monitoreo centralizado que permitan la recolección, análisis y correlación de eventos de seguridad en tiempo real.

Describir el procedimiento que se trabajará para implementar módulos de auditoría(Logs) (los que apliquen) en los sistemas de información que se encuentran bajo lagobernabilidad del Ministerio de Minas, teniendo en cuenta los estándares que establece lo siguiente: “Se adopta la Política General de Seguridad y Privacidad dela Información, la Política de Tratamiento y Protección de Datos Personales, la Política de Continuidad del Negocio, la Política ante Recuperación ante Desastres TIC y las Políticas de Seguridad y Privacidad de la Información”. (Resolución 40046 del 01-11-2023)

Para el informe del segundo trimestre del año 2025, se establecen los diferentes sistemas de información (SI) que están determinados bajo una caracterización de “consulta” y otros de “auditoría". El paso siguiente es que bajo el perfilamiento del grupo TIC del MINENERGÍA, se defina si dicha caracterización es correcta para usarla herramienta de auditoria en cada uno de los procesos (necesarios) y tener resultados para su posterior análisis. Para más información de la división de estos SI, remitirse al responsable de seguridad de la información a cargo.

Se establece la hoja de ruta del proceso de auditoria apara losSistemas de información SI y de los desarrollos pertinentes:

Imagen [11]. Hoja de ruta para procesos de auditoria en los SI.

Teniendo en cuenta lo anterior, se tiene en la actualidad 16 sistemas de información con módulo de auditoria (a continuación, se muestran algunos ejemplos del proceso en especial los nuevos implementados en desarrollo de aplicaciones de open source y establecimiento de datos de los Logs, sin embargo, no se muestra la lista completa ya que es de carácter público reservado, esto con fines de confidencialidad y asuntos internos, para más información remitirse al personal de seguridad de la información.

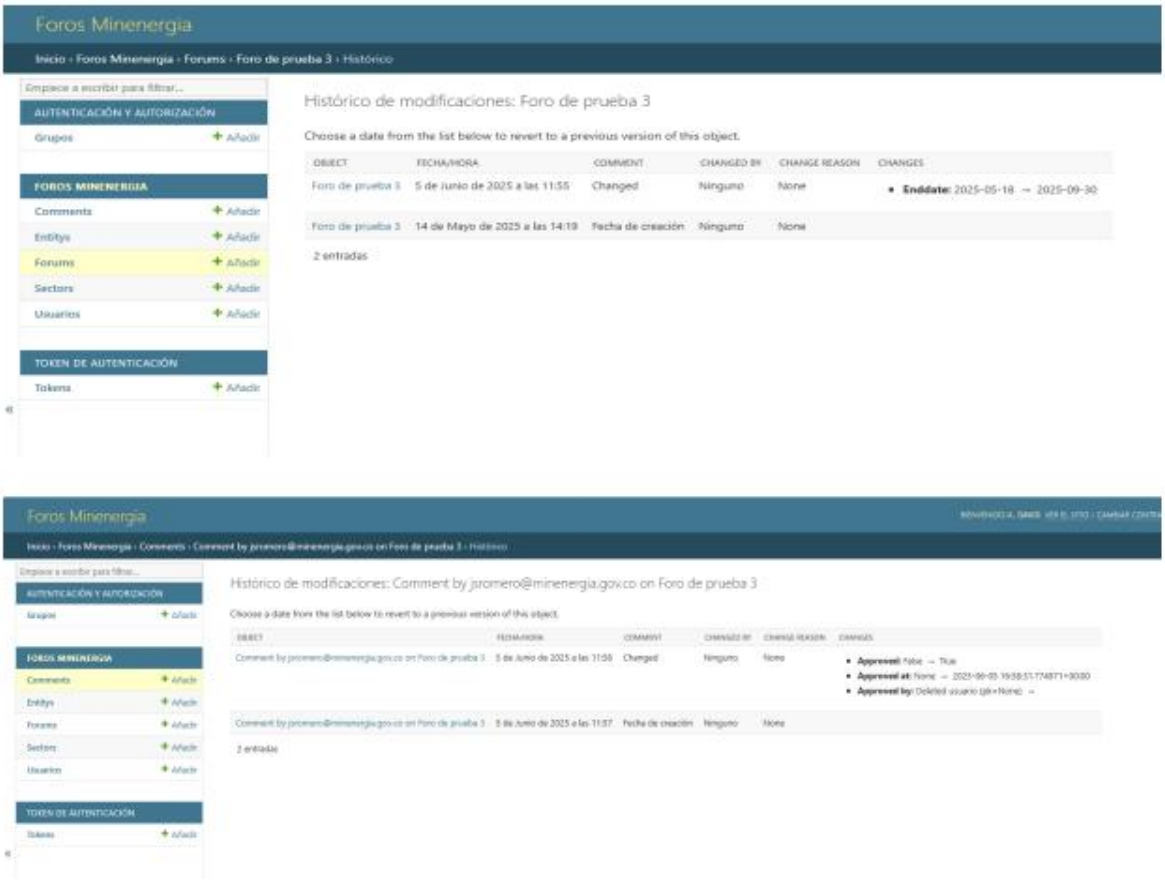


Imagen [12]. Ejemplo de auditoria SI Servicio al ciudadano y foros, listado de acceso por usuarios (los usuariosexpuestos son casos de ejemplo no correspondiente a credenciales reales).

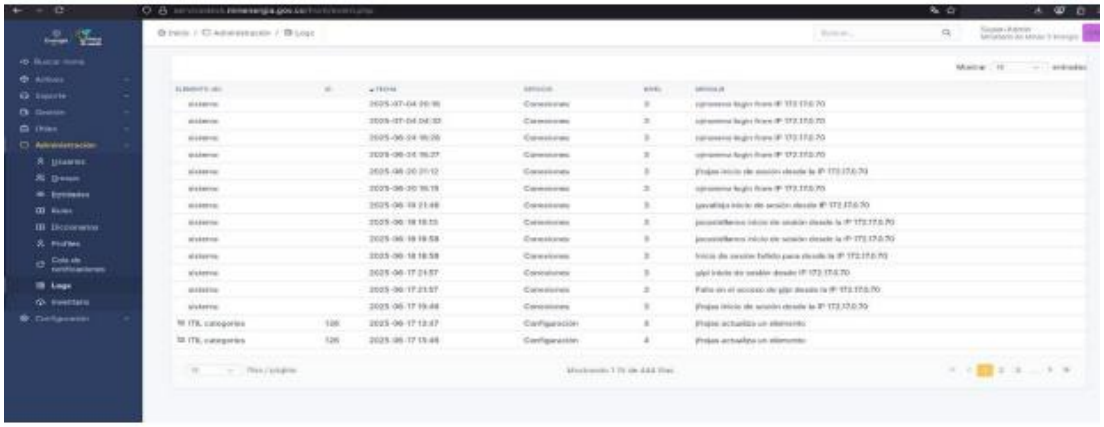


Imagen [13]. Ejemplo de auditoria SI GLPI, filtrado (los usuarios expuestos son casos de ejemplo no correspondiente a credenciales reales).

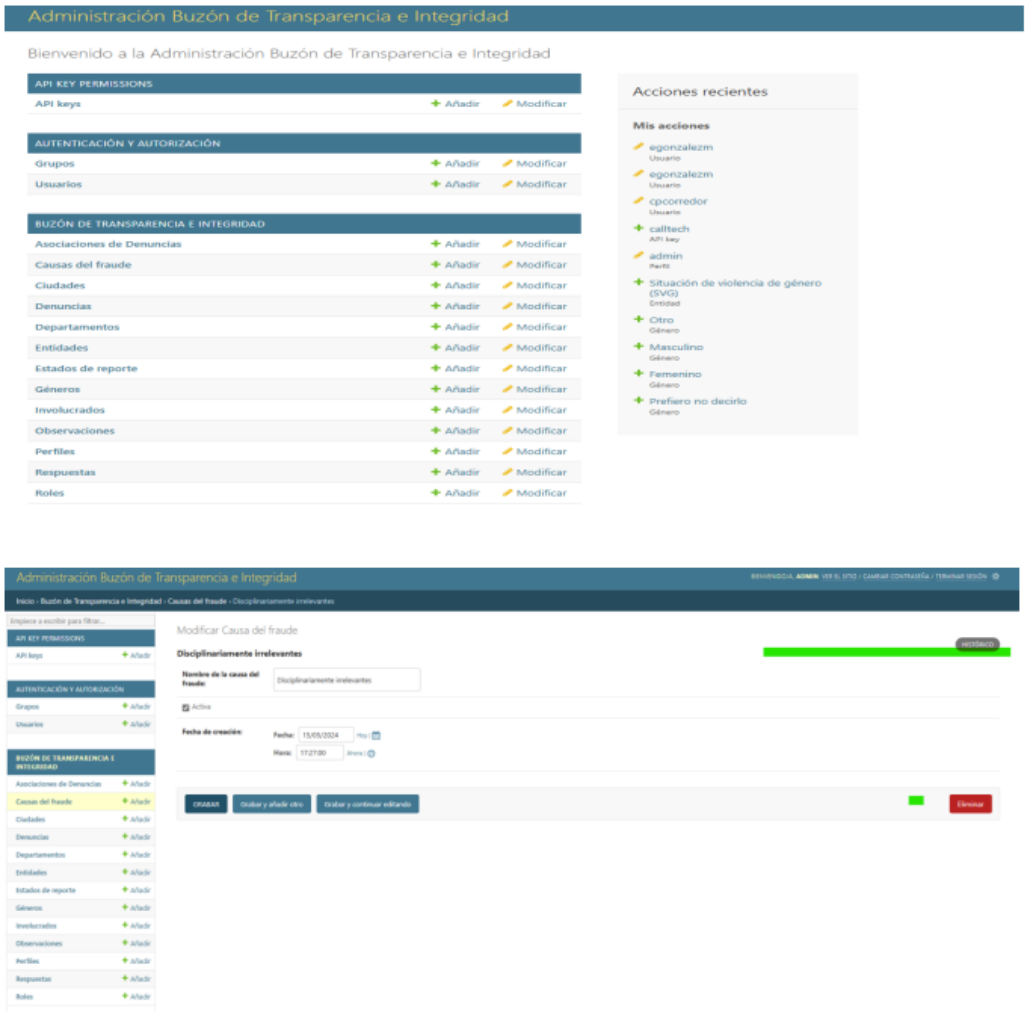


Imagen [14]. Ejemplo de auditoria Buzón de integridad y transparencia(los usuarios expuestos soncasos de ejemplo no correspondiente a credenciales reales).

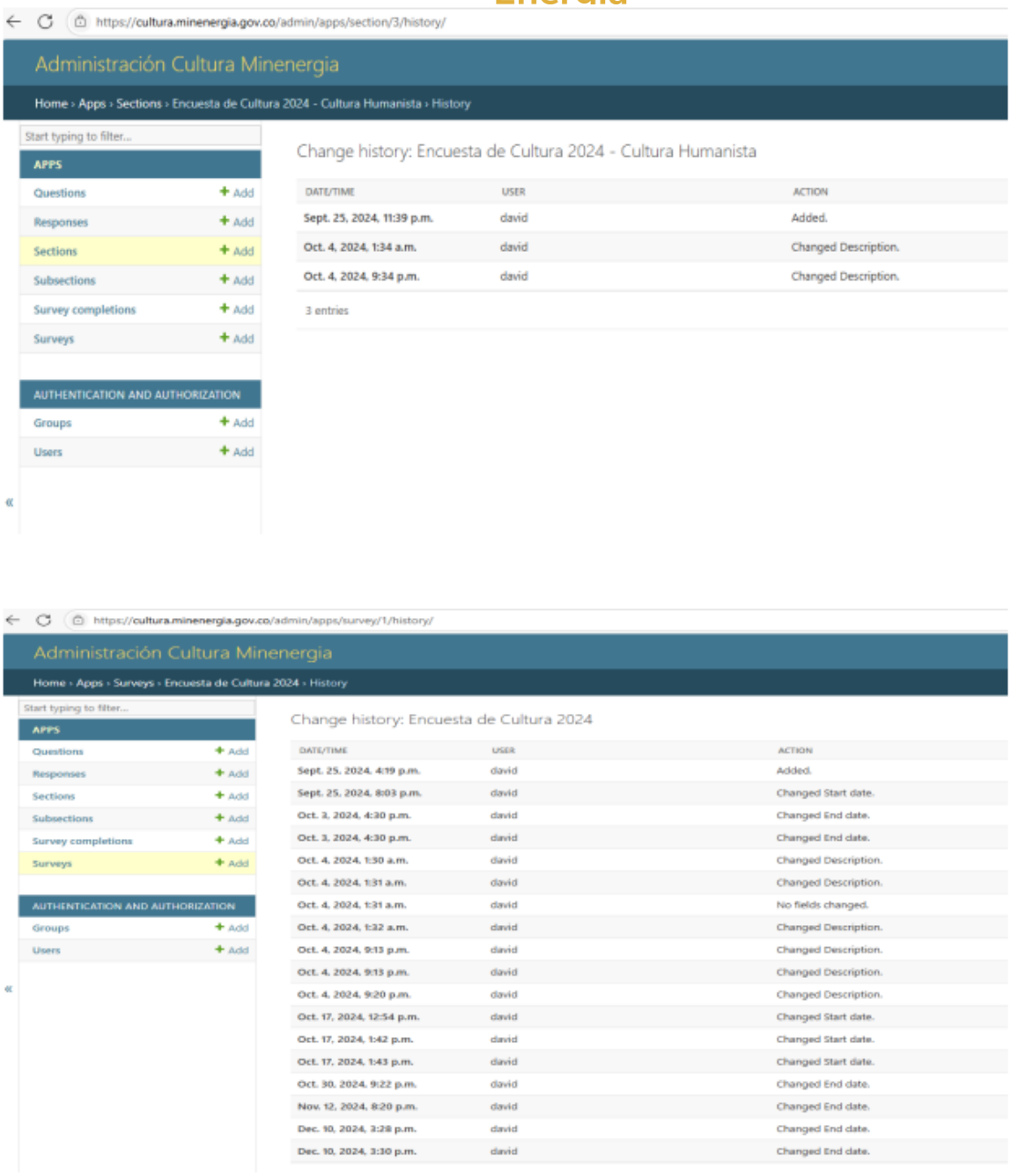


Imagen [15]. Ejemplo de auditoria encuesta de medición cultura organizacional, (los usuarios expuestosson casos de ejemplo no correspondiente a credenciales reales).

El módulo de auditoría "site-history" de Wagtail es una herramienta esencial para los administradores que necesitan realizar un seguimiento de los cambios realizados dentro de su sitio web. Este módulo registra una amplia variedad de acciones en el sitio, incluidas modificaciones de contenido, creaciones y eliminaciones de páginas. Al ofrecer una visión clara y detallada del historial de modificaciones, "site-history" es invaluable para la gestión de la seguridad, la auditoría de contenido y la resolución de problemas.

Es importante destacar que se debe formalizar el procedimiento de implementacióndel módulo de auditoría para los sistemas de información del Ministerio de Minas y Energía con herramientas óptimas y pragmáticas, para mayor seguridad de los mismos e iniciar con la fase de planeación con el equipo de trabajo competente en aras de establecer una productividad conjunta en la estructuración del módulo de auditoría de los sistemas de información a los que aplique.

NOTA: Los sistemas de información anteriormente relacionados cuentan con elementos y/o componentes de auditoría no necesariamente funcionalidades específicas que sean utilizadas como módulo auditor, sin embargo, lo citado cuenta con los componentes correspondientes que evidencian el seguimiento que se realiza dentro de cada sistema.

Riesgo R14 Realizar las tareas y actividades de backup, respaldo ydisposición acorde con plan de programación y/o solicitudes puntuales.

Actividad 2: Implementar métricas clave como tasas de éxito/falla, capacidad de almacenamiento disponible y tiempos de recuperación, asegurando que el sistema no se sature y opere de manera óptima, esto determinará si se continua con esta herramienta de respaldo o si se debe reemplazar por otra que cumpla los estándares necesarios.

Durante el segundo trimestre de 2025, se continuó fortaleciendo la gestión de respaldos mediante la plataforma Arcserve UDP Backup, consolidando avances significativos en términos de eficiencia, recuperación de espacio, y continuidad operacional de los procesos de respaldo. Estas actividades responden a la necesidad de mantener un entorno de respaldo robusto, confiable y alineado con los objetivos de continuidad del negocio, mitigando riesgos asociados a la saturación de almacenamiento, fallos en la recuperación y represamiento de datos críticos.

Este informe detalla los avances alcanzados en este periodo, con énfasis en la consolidación del respaldo a disco, la culminación de la depuración de puntos de restauración históricos, el reinicio de respaldos críticos, y la ejecución del Backup Full Granular a Cinta como parte de la estrategia de redundancia y resiliencia en almacenamiento.

Detalle de actividades realizadas

1. **Consolidación de la herramienta Arcserve UDP Backup con 204 Servidores Respaldados a Disco**

Durante este trimestre, se mantuvo la operación activa y continua del sistema de respaldo mediante la herramienta Arcserve UDP Backup, alcanzando la consolidación del respaldo de 204 servidores críticos a disco. Esta cifra refleja un ajuste respecto al primer trimestre, enfocado en mantener únicamente los servidores con respaldo activo, eficiente y dentro de la política de retención establecida.

La priorización de servidores críticos y la depuración de elementos obsoletos han contribuido a optimizar la operación de respaldo, liberando recursos del sistema y mejorando los tiempos de procesamiento.

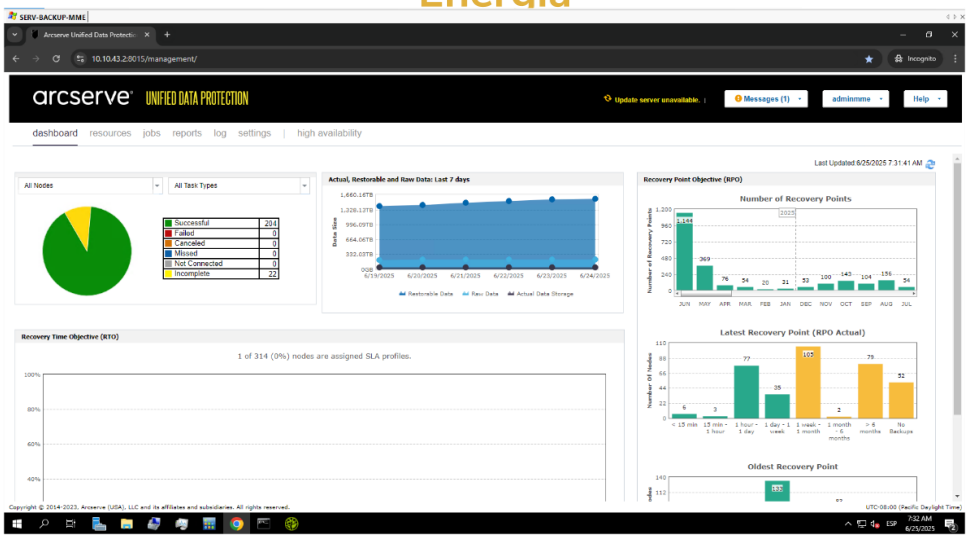


Imagen [16]. Proceso de ejecución de backups segundo trimestre 2025

2. Culminación de la depuración de los puntos de restauración históricos

Una de las actividades clave del trimestre fue la conclusión del proceso de depuración de puntos de restauración históricos almacenados en la partición x:\UDPData1. Gracias a esta labor, se logró liberar un total de 26.3TB, pasando de 1.5TB disponibles a 26.8TB de espacio libre. Esta optimización del almacenamiento fue fundamental para la sostenibilidad del sistema y para permitir la reanudación de procesos represados.

La depuración completa permitió eliminar respaldos obsoletos que estaban generando saturación, y con ello, se logró estabilizar el entorno y garantizar la disponibilidad de espacio para los backups en curso.

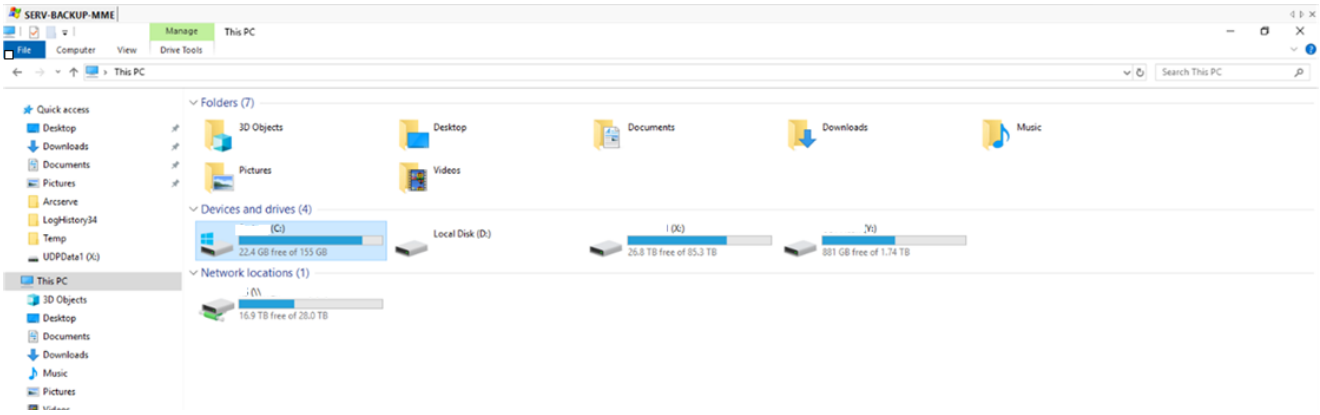


Imagen [17]. Restauración de sistemas y liberación de memoria segundo trimestre 2025.

3. **Relanzamiento de backups críticos (correos y bases de datos)**

Con el espacio liberado en el punto anterior, se logró relanzar exitosamente los procesos de respaldo de correos electrónicos y bases de datos que se encontraban represados debido a la saturación del almacenamiento. Estas operaciones fueron fundamentales para garantizar la protección de información sensible y estratégica, incluyendo comunicaciones institucionales y bases transaccionales.

Esta reactivación oportuna contribuye a mantener la continuidad operativa de los sistemas de información más críticos para la entidad.

4. **Ejecución del Backup Full granular a cinta**

Como parte del plan estratégico de recuperación ante desastres, el 06 de junio de 2025 se inició la ejecución del Backup Full Granular a Cinta, que busca generar una copia física adicional del respaldo actual.

Hasta la fecha de corte del presente informe, se han procesado 11.6TB de un total estimado de 58.5TB, lo que representa un avance del 19.8% en 18 días de ejecución continua. Con base en este ritmo, se estima que el proceso finalizará en aproximadamente 94 días, cumpliendo así con los tiempos previstos para la finalización de este respaldo de largo plazo.

Esta actividad fortalece la política de redundancia y almacenamiento fuera de línea, mitigando el riesgo de pérdida total de información ante eventos catastróficos o ataques dirigidos.

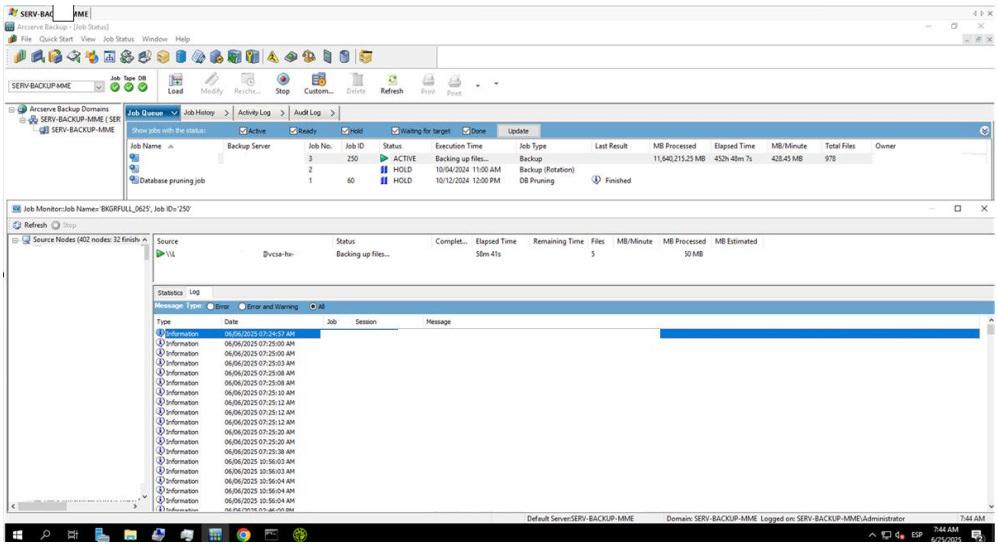


Imagen [18]. Proceso de ejecución de backups full granular a cinta , segundo trimestre 2025

Evaluación del desempeño de la herramienta

Durante el trimestre, se mantiene el seguimiento a las métricas definidas en el trimestre anterior, con resultados favorables:

- **Tasa de éxito de respaldos**: Se ha incrementado tras la depuración y relanzamiento de procesos.
- **Espacio disponible**: La recuperación de 26.3TB permite operar con holgura durante los siguientes ciclos de respaldo.
- **Tiempos de recuperación**: Se mantienen dentro de los rangos establecidos, al contar con respaldos organizados y depurados.

Estas métricas permiten confirmar que la herramienta Arcserve UDP Backup continúa siendo adecuada para las necesidades de respaldo de la entidad, aunque se recomienda mantener la vigilancia constante sobre los tiempos de respaldo a cinta y posibles cuellos de botella durante la ejecución.

Conclusión

El segundo trimestre de 2025 ha representado un punto de consolidación en la estrategia de respaldo de la organización. Se ha completado exitosamente la depuración de respaldos históricos, recuperando una cantidad significativa de espacio crítico, se reactivaron respaldos de datos sensibles, y se inició el Backup Full Granular a Cinta como medida complementaria de resiliencia.

Estos avances demuestran una madurez operativa creciente del sistema de respaldo, y reafirman el compromiso con la protección de la información institucional. Se recomienda continuar con el monitoreo permanente de las métricas clave y mantener el cronograma de ejecución de respaldo a cinta hasta su culminación prevista.

R23: Procedimiento Gestión de Continuidad y Recuperación de los Servicios de Informática y Comunicaciones. Ausencia de DRP actualizado.

Actividad 1: Evaluar la infraestructura tecnológica actual y actualizar el DRP con base en las mejores prácticas y estándares

Durante el segundo trimestre del año 2025, se han mantenido avances sustanciales en el fortalecimiento de la estrategia de continuidad del negocio del Ministerio de Minas y Energía, especialmente en lo relacionado con la actualización del Plan de Recuperación ante Desastres (DRP) y la implementación de un centro de datos alterno. Estas acciones se desarrollan en línea con las recomendaciones surgidas del análisis técnico realizado en el primer trimestre y con las mejores prácticas internacionales en gestión de la infraestructura crítica de TI.

- Avances en el fortalecimiento de la infraestructura de respaldo

1. Nueva solución de backup en proceso de adquisición:

Se encuentra en curso el proceso contractual para la adquisición de una herramienta avanzada de respaldo que incluye soporte para almacenamiento tanto en disco como en cinta, con características de inmutabilidad y replicación automática hacia el centro de datos alterno. Esta solución permitirá fortalecer los esquemas de recuperación de información frente a eventos de pérdida, corrupción o ataque a la infraestructura digital, y garantiza el cumplimiento de principios como la integridad, disponibilidad y resiliencia de los datos críticos.

2. Migración del centro de datos alterno a un esquema de colocation externo:

En concordancia con los resultados de las visitas técnicas realizadas en el primer trimestre, se avanza en la contratación de un servicio de colocation externo que cumpla con los requisitos mínimos establecidos por el Ministerio y las certificaciones internacionales aplicables (por ejemplo, TIER III). Este traslado permitirá mejorar los niveles de disponibilidad, escalabilidad, redundancia y seguridad física/lógica de la infraestructura de respaldo. Actualmente, este componente también se encuentra en proceso para ser formalmente incluido en el Sistema Integrado de Planeación (SIP).

3. Mantenimiento preventivo y correctivo de infraestructura y seguridad:

Se vienen ejecutando acciones coordinadas con los proveedores actuales de infraestructura tecnológica y seguridad, tanto a nivel físico como lógico. Estas incluyen mantenimientos preventivos sobre sistemas de energía, climatización, servidores y dispositivos de red, así como ajustes de

seguridad perimetral, con el objetivo de asegurar la estabilidad y continuidad de los servicios que soportan las operaciones misionales de la entidad.

- Etapas ejecutadas de la estrategia de implementación del DRP

La iniciativa ha avanzado en varias fases del ciclo de implementación del DRP, siguiendo una hoja de ruta estructurada:

Evaluación de necesidades y diagnóstico:
Culminado en el primer trimestre, mediante visitas técnicas, análisis comparativo de oferentes, e inventario de activos críticos.

Planificación y diseño de la solución:
Se ha elaborado una propuesta técnica preliminar, actualmente en proceso de ajuste y afinamiento, la cual establece los criterios técnicos, operativos y de seguridad para la operación del centro de datos alterno, así como las bases para la actualización del DRP.

Etapa contractual en curso:
La iniciativa se encuentra en proceso contractual, superando las fases de planeación y formulación del Anexo Técnico inicial. Actualmente se encuentra en perfeccionamiento, avanzando hacia la etapa de adjudicación y ejecución conforme al cronograma establecido.

Tabla 3
Inventario centro de datos alterno de la entidad (para mayor información remitirse al líder de la infraestructura del Grupo TICS).

Marca	Modelo	Serie (Parcial)	Tipo de Equipo	Código Interno	Altura (Rack Units)
CISCO	UCS-FI-XXX	[CENSURADO]	Fabric Interconnect	S/P	1RU
CISCO	UCS-FI-XXX	[CENSURADO]	Fabric Interconnect	S/P	1RU
CISCO	WS-C2960X-4XXXX-L	[CENSURADO]	Switch	S/P	1RU
CISCO	UCSC-C240-XXXX	[CENSURADO]	Server Host	151861	2RU
CISCO	HXAF 240C-XXX V02	[CENSURADO]	Server Host	151862	2RU
CISCO	HXAF 240C-XXX V02	[CENSURADO]	Server Host	151862	2RU
CISCO	HXAF 240C-XXX V02	[CENSURADO]	Server Host	S/P	2RU
FORTINET	XXXX	[CENSURADO]	Firewall	151875	2RU

4.4 GESTIÓN DE POLÍTICAS Y PROCEDIMIENTOS

Durante el segundo trimestre del 2025, se consolidaron avances significativos en el fortalecimiento del marco normativo e institucional de la seguridad y privacidad de la información, en concordancia con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), el Sistema de Gestión de Seguridad de la Información (SGSI), la Política de Confianza y Seguridad Digital, y la Resolución 40646 de 2023.

Uno de los hitos más relevantes fue la finalización del proceso de revisión de la Política de Uso Responsable de Inteligencia Artificial (IA), la cual establece los principios éticos, técnicos y de gobernanza aplicables a soluciones de IA implementadas en el Ministerio. Este documento será parte integral del marco de políticas institucionales y servirá como guía transversal para el desarrollo, adquisición y uso de sistemas inteligentes, garantizando el respeto por los derechos fundamentales y la mitigación de riesgos asociados a decisiones automatizadas.

En cuanto al sistema SICOM, se realizó un ajuste estratégico en la gestión documental de la política de tratamiento de datos personales. En lugar de emitir una política específica para SICOM (lo cual generaría redundancia normativa) se decidió mantener la referencia a la política institucional del Ministerio, tal como lo establece la Resolución 40646. No obstante, para asegurar el cumplimiento de los requerimientos operativos del sistema, se inició la modificación del Manual del Usuario del Sistema SICOM, el cual incorporará una sección detallada sobre la aplicación de la política de privacidad en dicho entorno, con énfasis en su uso, responsabilidades de los usuarios y tratamiento de datos sensibles, conforme a la Ley 1581 de 2012 y su reglamentación.

De forma paralela, se logró un avance sustancial en el proceso de gestión de incidentes de seguridad de la información, particularmente con la definición de la plantilla oficial de informe de incidentes cibernéticos, la cual ya fue remitida para su revisión y aprobación final. Esta herramienta permitirá estandarizar la documentación de incidentes, mejorando la trazabilidad, el análisis forense y la toma de decisiones basada en evidencias.

Finalmente, se avanzó en la estructuración del proceso de gobernanza de dispositivos tecnológicos, con el objetivo de establecer un modelo de control centralizado sobre los equipos entregados a las distintas dependencias. En este sentido, se diseñó un procedimiento preliminar que establece que todo equipo o dispositivo de cómputo (como portátiles, estaciones de trabajo o periféricos) deberá ser gestionado y validado por la Dirección TIC antes de su asignación, permitiendo así un control más riguroso sobre los activos, su ciclo de vida, configuración de seguridad base, y trazabilidad operativa dentro del ecosistema institucional.

Estos avances se enmarcan dentro del proceso de mejora continua del SGSI, y preparan el camino para abordar nuevos retos en el segundo semestre, particularmente en lo relacionado con la implementación de controles de seguridad sobre sistemas legados, la gestión de terceros y la integración de herramientas de gobierno digital para el monitoreo de cumplimiento normativo en tiempo real.

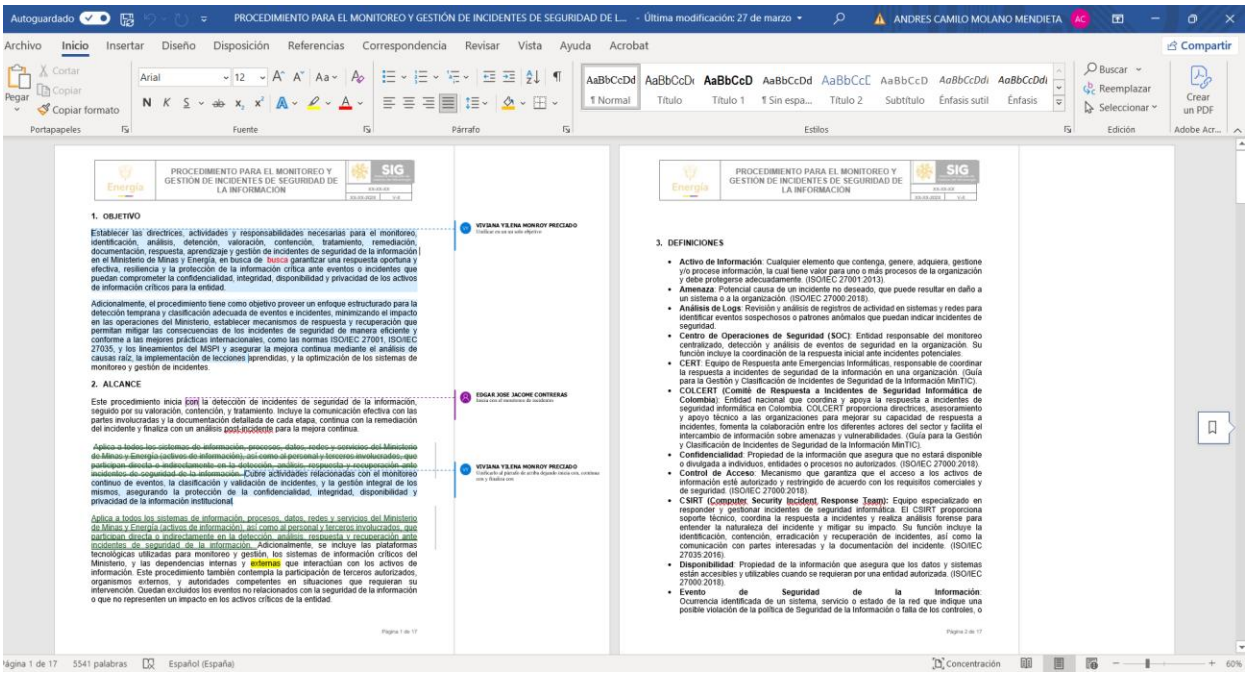


Imagen [19]. Control de cambios y observaciones del procedimiento de monitoreo y gestión de incidentes de seguridad de la información.

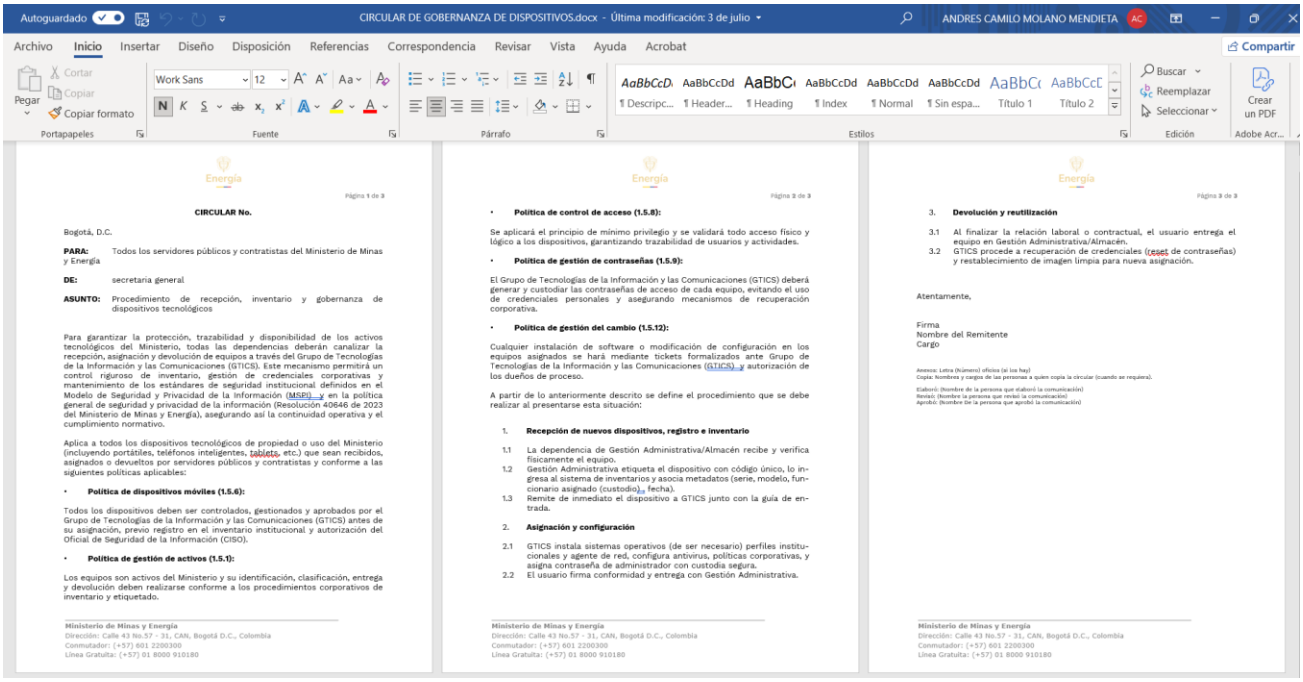


Imagen [20]. Circular estructurada para el manejo y gobernanza de la los dispositivos TI .

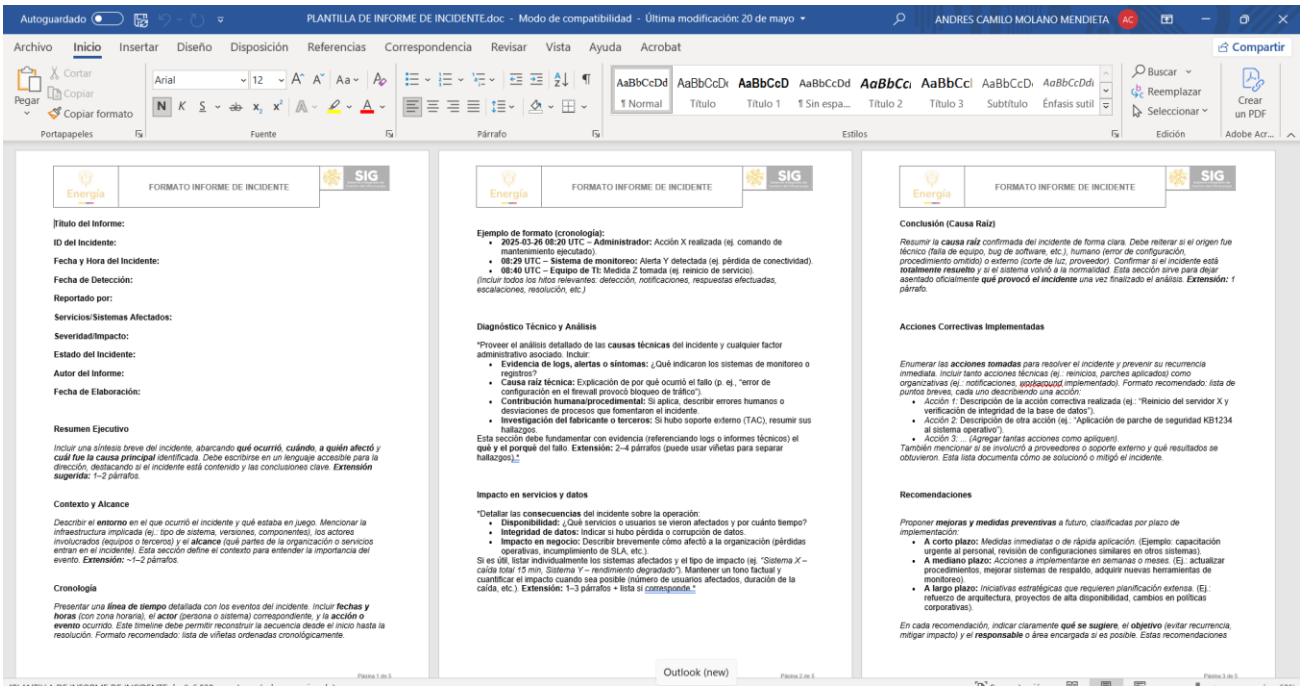


Imagen [21]. Plantilla de informe de gestión de incidentes.

4.5 GESTIÓN DE RECURSOS DE SEGURIDAD

Conforme al análisis del contexto actual de la entidad, tanto en su dimensión externa marcada por la evolución de amenazas cibernéticas emergentes, como los ataques dirigidos, el ransomware y la ingeniería social como en su dimensión interna, donde persisten retos en materia de protección de datos, madurez en seguridad de la información y cultura organizacional en ciberseguridad, se ha definido una hoja de ruta estratégica de proyectos prioritarios para la vigencia 2025. Estos proyectos están diseñados para cerrar brechas críticas de seguridad, mejorar los niveles de preparación ante incidentes, y fortalecer los pilares institucionales de ciberdefensa, ciberseguridad y ciberresiliencia, en línea con las directrices del Gobierno Digital y las políticas nacionales de confianza digital.

Tabla 4.
Proyectos a implementar vigencia 2025

PROYECTO
Contratar los servicios especializados para realizar análisis de vulnerabilidades, ethical hacking e pentesting social a la infraestructura tecnológica del Ministerio de Minas y Energía
Implementar soluciones de seguridad y privacidad de la información que incorpore procesos, talento humano y tecnología para dar cumplimiento a los lineamientos de MINTIC.
Implementar un Csirt para responder a incidentes de seguridad que incorpore procesos, recurso humano y tecnología para dar cumplimiento a la política de gobierno digital en el habilitador de seguridad digital.
Implementar esquemas de continuidad de negocio (BCP — Business Continuity Plan) y plan de recuperación de desastres (DRP) sectorial, que incorpore procesos, recurso humano y tecnología
Adquirir herramienta de seguridad para el monitoreo de la red, para detección de amenazas en tiempo real en el Ministerio de Minas y Energía (SOC)
Renovar el licenciamiento de firewall local y adquisición de firewall de aplicaciones web (WAF) para proteger las aplicaciones web y monitorizar el tráfico HTTP del centro de datos alterno del Ministerio de Minas y Energía

Durante el segundo trimestre de 2025, el Ministerio de Minas y Energía continuó avanzando de manera decidida en la implementación de la hoja de ruta estratégica definida para el fortalecimiento de los recursos de seguridad de la información, conforme a las directrices de la Resolución 40646 de 2023, la Política de Confianza y Seguridad Digital, el CONPES 3995 de 2020 y el Modelo de Seguridad y Privacidad de la Información (MSPI). Las iniciativas priorizadas integran componentes tecnológicos, humanos y procesales que permiten robustecer la capacidad institucional frente a amenazas cibernéticas, garantizar la disponibilidad de la infraestructura crítica y fortalecer la gobernanza sectorial en ciberseguridad.

1. Plataforma de Backup Institucional

Se avanzó en la fase precontractual para la adquisición e implementación de una solución avanzada de respaldo de la información, que cubre servicios y aplicaciones críticos del Ministerio. Hasta la fecha se han completado las etapas de evaluación de necesidades, diseño de la solución y planificación, y se cuenta con un anexo técnico, formato económico y formato de información a proveedores, actualmente en proceso de ajuste y afinamiento. Esta solución contempla funcionalidades de inmutabilidad, respaldo en disco y cinta, y replicación automática hacia el centro de datos alterno, con el objetivo de garantizar la resiliencia, disponibilidad e integridad de los datos institucionales ante eventos disruptivos.

2. Centro de Monitoreo Sectorial

La iniciativa para implementar un Centro de Monitoreo Sectorial, que integrará los servicios de sala de monitoreo y control, CSIRT sectorial, soluciones DRP/CDA, y tecnologías emergentes, se encuentra también en etapa precontractual. Se han culminado las fases de evaluación de necesidades y diagnóstico, así como la planificación y diseño inicial, y se dispone de un anexo técnico preliminar en proceso de revisión y ajuste. Esta infraestructura será un habilitador estratégico para la gestión centralizada de la ciberseguridad sectorial, permitiendo la detección oportuna de amenazas, la coordinación de respuesta ante incidentes y el fortalecimiento de capacidades compartidas entre entidades del sector minero-energético.

Cabe resaltar que el equipo técnico del CSIRT sectorial se integró a esta iniciativa de inversión, consolidando esfuerzos técnicos, presupuestales y operativos bajo una visión unificada de defensa digital sectorial.

3. Análisis de Vulnerabilidades, Ethical Hacking y Pentesting Social

Este proyecto se encuentra en etapa precontractual para su ejecución mediante convenio interadministrativo durante el tercer trimestre de 2025. Su propósito es evaluar de forma proactiva la postura de seguridad de la infraestructura tecnológica del Ministerio, mediante pruebas controladas que permitan identificar vulnerabilidades y debilidades explotables, especialmente en entornos

expuestos a internet, sistemas misionales y servicios críticos. Esta iniciativa también hace parte del marco de acciones fundacionales del CSIRT sectorial, contribuyendo a la consolidación de capacidades de análisis preventivo, gestión de riesgos y respuesta a incidentes.

4. Fortalecimiento de la Estrategia de Continuidad del Negocio (DRP)

Durante este trimestre, se consolidaron importantes avances en la actualización e implementación del Plan de Recuperación ante Desastres (DRP), enmarcados en el proceso integral de aseguramiento de la continuidad operativa y protección de la infraestructura crítica de TI. Los principales logros incluyen:

Adquisición de solución de backup: En proceso contractual, incorpora almacenamiento híbrido (disco y cinta), replicación automatizada e inmutabilidad de respaldos, asegurando cumplimiento de principios como integridad, disponibilidad y resiliencia.

Migración del centro de datos alterno hacia un esquema de colocation externo: Se avanza en la contratación de un proveedor con infraestructura certificada (por ejemplo, TIER III), lo cual permitirá elevar los niveles de seguridad física/lógica, redundancia, escalabilidad y disponibilidad.

Mantenimientos preventivos y correctivos de infraestructura crítica: Se ejecutan en coordinación con los proveedores actuales, e incluyen mejoras en energía, climatización, conectividad, seguridad perimetral y dispositivos de red.

En términos metodológicos, la estrategia de implementación del DRP ha superado las fases de evaluación de necesidades, diagnóstico técnico, planificación y diseño de solución, y actualmente se encuentra en fase contractual, con el anexo técnico en proceso de perfeccionamiento para su posterior adjudicación y ejecución.

5. SEGUIMIENTO PLAN DE ASEGURAMIENTO Y EVALUACIÓN DE LA IMPLEMENTACIÓN Y MANTENIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN

5.1 GESTIÓN DE INDICADORES

La gestión de indicadores constituye una herramienta clave para evaluar la eficacia, eficiencia y efectividad de las políticas, procedimientos y controles establecidos en el marco del Sistema de Gestión de Seguridad de la Información (SGSI) del Ministerio de Minas y Energía. Esta práctica permite no solo monitorear el cumplimiento normativo, sino también identificar oportunidades de mejora continua, en concordancia con los principios establecidos en la Guía Técnica No. 9 del Modelo de Seguridad y Privacidad de la Información (MSPI) y las normas internacionales ISO/IEC 27001:2022 y ISO/IEC 27004:2022.

Durante el segundo trimestre de 2025, se realizó una revisión de los indicadores previamente definidos en la vigencia anterior, con el objetivo de priorizar aquellos que mejor reflejaran la madurez del sistema, la capacidad de respuesta institucional y el impacto en la cultura de seguridad. Tras una evaluación conjunta con los equipos técnicos y el responsable de seguridad de la información, se seleccionaron cinco indicadores clave para su seguimiento durante el año. Esta selección responde tanto a las prioridades institucionales como a la necesidad de contar con métricas claras que reflejen los avances logrados.

A continuación, se presenta la tabla con los indicadores seleccionados, sus descripciones, fórmulas y los resultados correspondientes al segundo trimestre de 2025:

Tabla 5
Resultado de indicadores de seguridad de la información

Indicador	Definición	Fórmula	Meta	Meta	Resultado 2 trimestre	Actividad
SGIN01	Organización de Seguridad de la Información	Mide el nivel de compromiso institucional con la definición formal de roles y responsabilidades en seguridad de la información.	(Roles definidos / Roles requeridos) * 100	80%-90% satisfactorio, 100% sobresaliente	**100%** (3/3)	Se definieron formalmente los cargos de CISO mediante la designación de la responsabilidad por parte de la coordinación del grupo TICS.

SGIN03	Tratamiento de eventos de seguridad	Evalúa la eficiencia en la gestión de los incidentes de seguridad detectados.	(Eventos tratados / Eventos reportados) * 100	80%-90% satisfactorio, 100% sobresaliente	**100%** (1/1)	3 Incidentes detectados, reportados y mitigados según los tiempos establecidos, están en proceso de aprobación por parte del CISO y la coordinación de grupo TICS para el envío a a la SIC.
SGIN16	Implementación de controles	Mide el grado de implementación de controles de seguridad según el plan de tratamiento de riesgos.	(Controles implementados / Controles planificados) * 100	75%-80% mínimo, 100% sobresaliente	**60%** (4/7)	Una actividad de control por cada riesgo fue implementada en este trimestre. Ver informe de seguimiento.
SGIN15	Disponibilidad de servicios críticos (SICOM)	Porcentaje de tiempo que los sistemas críticos estuvieron operativos según los Acuerdos de Nivel de Servicio (ANS).	(Tiempo disponible / Tiempo planificado) * 100	>99% sobresaliente	**100%**	La disponibilidad del sistema SICOM se mantuvo al 100%. Ver informe del proveedor.
SGIN04	Sensibilización en seguridad de la información	Evalúa la efectividad del plan de sensibilización mediante actividades ejecutadas frente a las programadas.	(Eventos realizados / Eventos programados) * 100	80%-90% satisfactorio, 100% sobresaliente	**100%** (4/4)	Proceso de ethical hacking, Ejercicio de ingeniería social pishing 3 sesiones Sensibilización y capacitación

El resultado de los indicadores seleccionados evidencia un desempeño sobresaliente durante el primer trimestre, cumpliendo al 100% con las metas propuestas en todos los frentes evaluados. Este desempeño refleja el compromiso de la entidad con el fortalecimiento de su SGSI, la implementación oportuna de controles, la estructuración formal de roles de seguridad y la eficiencia en la atención de incidentes.

Para los próximos trimestres, se dará continuidad al monitoreo de estos cinco indicadores con base en el cronograma operativo del SGSI. Además, se proyecta la integración de estos resultados a la herramienta de gestión ERAMBA, con el fin de automatizar la recolección, seguimiento y análisis de

indicadores, alineando esta función con los procesos de auditoría interna, planificación estratégica y evaluación de desempeño institucional en materia de ciberseguridad.

5.2 GESTIÓN DE VULNERABILIDADES.

Durante el primer trimestre del año 2025, y conforme a las actividades establecidas en el Plan de Seguridad y Privacidad de la Información, se dio inicio a la implementación del repositorio institucional de seguimiento a vulnerabilidades, el cual opera mediante la herramienta de gestión colaborativa Planner, integrada a la suite de productividad de la entidad. Este repositorio tiene como finalidad centralizar, documentar y dar trazabilidad a todas las actividades de detección, análisis, tratamiento y cierre de vulnerabilidades técnicas, garantizando así un control sistemático y continuo sobre las debilidades que puedan afectar la infraestructura tecnológica y los sistemas de información críticos del Ministerio de Minas y Energía.

Como parte del proceso, a partir del 3 de marzo de 2025, se definieron los sistemas de información priorizados para el análisis de vulnerabilidades, conforme a criterios de criticidad técnica, funcional y operativa establecidos por el Grupo de Infraestructura Tecnológica. Esta priorización se basa en el nivel de exposición de los sistemas, su valor estratégico para la entidad, y su impacto potencial frente a incidentes de seguridad. Con este enfoque, se busca optimizar los recursos y asegurar la protección de los activos más sensibles, alineando esta actividad con los principios de gestión basada en riesgos y con los lineamientos de la norma ISO/IEC 27002:2022 en su sección de gestión de vulnerabilidades técnicas.

La siguiente tabla presenta el cronograma de ejecución para el análisis de vulnerabilidades de los sistemas priorizados, incluyendo fechas estimadas, responsables técnicos, y mecanismos de verificación y cierre. Esta actividad es complementaria a los controles definidos en el plan de tratamiento de riesgos y se articula con los demás componentes del Sistema de Gestión de Seguridad de la Información (SGSI), fortaleciendo así la postura institucional en ciberseguridad y aseguramiento digital.

Tabla 6
Cronograma de vulnerabilidades

APLICACIÓN	FECHA
IFX_repositoriobi	SEMANA 1
NORMATIVAMME	SEMANA 1
IFX_PORTAL_MME_HTTPS	SEMANA 1

Aula Virtual	SEMANA 1
Biblioteca	SEMANA 1
Suime 3 Fondo BEcas	SEMANA 1
IFX_WEBGLP	SEMANA 2
IFX_SISEG	SEMANA 2
GITLAB	SEMANA 2
IFX_SIPRIVADO	SEMANA 2
IFX_MESADEAYUDA	SEMANA 2
IFX_SERVICIOS	SEMANA 2
Directorio Activo	SEMANA 2
IFX_REPORTES_SISEG ENERGIA	SEMANA 3
IFX_GEOVISOR	SEMANA 3
IFX_EITI_COLOMBIA 179.1.211.170 172.17.10.125	SEMANA 3
SARA_	SEMANA 3
sith.minminas.gov.co_ifx	SEMANA 3
siveeic_http	SEMANA 3
siveic_https	SEMANA 3
siveic_3020	SEMANA 3
siveic_3010	SEMANA 3
Servidores Virtuales	SEMANA3
GRC	SEMANA 4
Portal_autogestion_accesos	SEMANA 4
Argopruebas	SEMANA 4
VIP_ARGOP	SEMANA 4
ARGO_CALIDAD	SEMANA 4
ARGO-DEV	SEMANA 4
argo_QA	SEMANA 4
SGP	SEMANA 4
Servidores Fisicos	SEMANA 4
SIGAME	SEMANA 5
Sara_TH	SEMANA 5
VIP_sisegdee	SEMANA 5
SISEGDH	SEMANA 5
NEON PRODUCCION	SEMANA 5

NEON_PRUEBAS	SEMANA 5
AVANZAME	SEMANA 5
AVANZAME_PROD	SEMANA 5
VIP_declaragas	SEMANA 6
VIP_geoserver	SEMANA 6
cargamap.minenergia	SEMANA 6
SARA_HTTPS	SEMANA 6
SERV_CREDITOBID	SEMANA 6
XROAD-QA	SEMANA 6
Mesa ayuda admin	SEMANA 6
VIP_ARGISENTERPRISE	SEMANA 7
VIP-ARGO-QA	SEMANA 7
sara 8480	SEMANA 7
GEONETWORK_PROD	SEMANA 7
SISEG-DH-PRUEBAS	SEMANA 7
JBPM-QA	SEMANA 7
TRANSPARENCIA_PROD	SEMANA 7
Energia evoluciona	SEMANA 7
SITH_PRUEBAS	SEMANA 8
CULTURA ENCUESTAS	SEMANA 8
WEBGLP 8081	SEMANA 8
WEBGLP 8082	SEMANA 8
OAAS VISOR CONFLICTOS	SEMANA 8
ASISTENTE VIRTUAL	SEMANA 8
ODKCENTRAL	SEMANA 8
TRAMITES	SEMANA 8
PGRD	SEMANA 8
pigccme.minenergia.gov.co	SEMANA 8
Intégrame	SEMANA 8
P8	Se validará al final que se hace con estas aplicaciones

Correspondencia SEERV MMECE Histórico	Se validará al final que se hace con estas aplicaciones
SIGME	Dejar de publicar

Para mayor detalle sobre el cumplimiento y los resultados obtenidos en los análisis de vulnerabilidades realizados durante el primer trimestre de 2025, se recomienda consultar directamente con el Oficial de Seguridad de la Información, quien centraliza y gestiona los informes técnicos correspondientes. Durante este periodo, se ejecutaron las actividades de escaneo y evaluación inicial de vulnerabilidades sobre los sistemas priorizados, conforme al cronograma establecido.

Se prevé que, en el segundo trimestre, se realicen las acciones de remediación necesarias con base en las recomendaciones emitidas en los informes, y posteriormente se llevará a cabo un retest técnico, con el objetivo de verificar y evidenciar de manera objetiva el cierre efectivo de las brechas identificadas. Este proceso permitirá validar la eficacia de las medidas aplicadas y alimentar el ciclo de mejora continua del SGSI.

Adicionalmente, los informes técnicos generados han sido remitidos a los oferentes o áreas responsables a través de correo electrónico institucional, junto con la estimación de los tiempos de remediación. Como parte del proceso formal de seguimiento, cada responsable debe registrar las acciones correctivas implementadas y su estado de avance en el formato oficial de gestión de vulnerabilidades, lo que permite mantener trazabilidad, control y evidencia documental ante auditorías internas o externas.

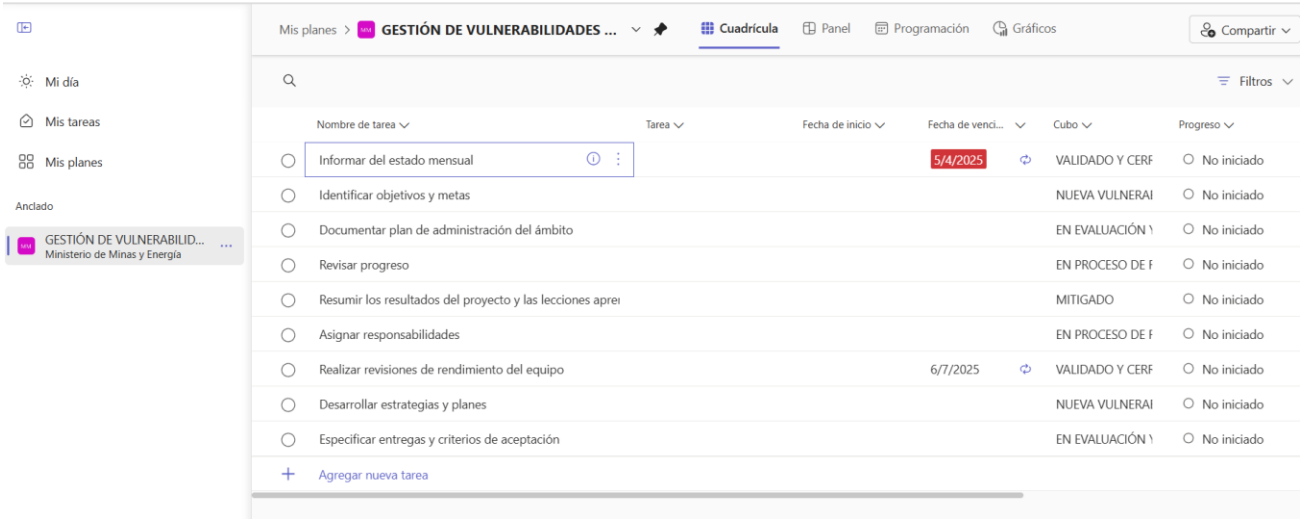


Imagen [21]. Seguimiento de gestión de vulnerabilidades con Planner.

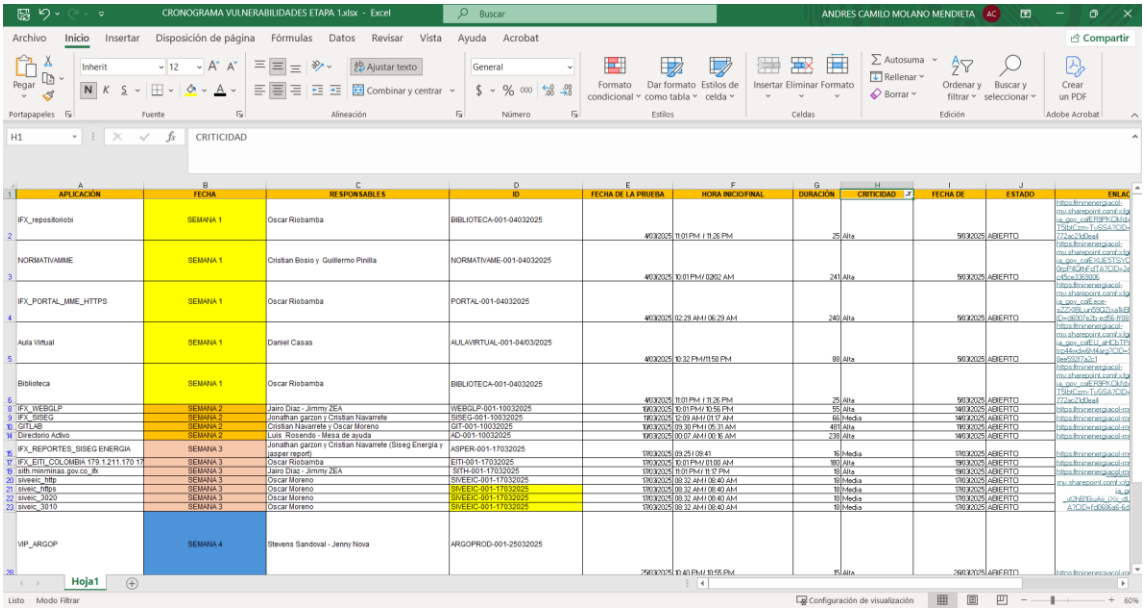
Energía	FORMATO REPORTE DE VULNERABILIDADES	SIG Sistema Integrado de Gestión del Minenergía V-3

DATOS DE LA PERSONA QUE NOTIFICA			
NOMBRE:		DEPENDENCIA:	
INFORMACIÓN SOBRE VULNERABILIDAD			
FECHA DE LA PRUEBA DE VULNERABILIDAD:		HORA DE INICIO / HORA FINAL:	DURACIÓN DE LA PRUEBA:
ID:	CRITICIDAD:	CVE/DESCRIPCIÓN:	FECHA DE DETECCIÓN:
ACTIVO AFECTADO:			FECHA DE CORRECIÓN: *Llenar por el responsable de remediación*
EVIDENCIA DE VULNERABILIDAD:			

Página 1

Imagen [22]. Formato de gestión de vulnerabilidades.

A partir de lo anteriormente descrito, en el segundo trimestre se lleva el control y seguimiento de las vulnerabilidades como se presenta a continuación:



APLICACIÓN	FECHA	RESPONSABLES	ID	FECHA DE LA PRUEBA	HORA INICIOFINAL	DURACIÓN	CRITICIDAD	FECHA DE	ESTADO	ENLAC
IFX_repositoriobi	SEMANA 1	Oscar Riobamba	BIBLIOTECA-001-04032025	4/03/2025	11:01 PM / 11:26 PM	25	Alta	5/03/2025	ABIERTO	
NORMATIVAMME	SEMANA 1	Cristian Bosio y Guillermo Pinilla	NORMATIV-AME-001-04032025	4/03/2025	10:01 PM / 03:02 AM	241	Alta	5/03/2025	ABIERTO	
IFX_PORTAL_MME_HTTPS	SEMANA 1	Oscar Riobamba	PORTAL-001-04032025	4/03/2025	02:29 AM / 06:29 AM	240	Alta	5/03/2025	ABIERTO	
Aula Virtual	SEMANA 1	Daniel Casas	AULAVIRTUAL-001-04/03/2025	4/03/2025	10:32 PM / 11:59 PM	88	Alta	5/03/2025	ABIERTO	
Biblioteca	SEMANA 1	Oscar Riobamba	BIBLIOTECA-001-04032025	4/03/2025	11:01 PM / 11:26 PM	25	Alta	5/03/2025	ABIERTO	
IFX_WEBGLP	SEMANA 2	Jairo Diaz - Jimmy ZEA	WEBGLP-001-10032025	10/03/2025	10:01 PM / 10:56 PM	55	Alta	14/03/2025	ABIERTO	
IFX_SIBEG	SEMANA 2	Jonathan garzon y Cristian Navarrete	SIBEG-001-10032025	10/03/2025	12:09 AM / 01:37 AM	68	Media	14/03/2025	ABIERTO	
GITLAB	SEMANA 2	Cristian Navarrete y Oscar Moreno	GIT-001-10032025	10/03/2025	03:30 PM / 05:31 AM	481	Alta	17/03/2025	ABIERTO	
Directorio Activo	SEMANA 2	Luis Rosendo - Mesa de ayuda	AD-001-10032025	10/03/2025	00:07 AM / 00:16 AM	238	Alta	14/03/2025	ABIERTO	
IFX_REPORTES_SISEG ENERGIA	SEMANA 3	Jonathan garzon y Cristian Navarrete (Siseg Energía y jasper report)	ASPER-001-17032025	17/03/2025	09:25 / 09:41	16	Media	17/03/2025	ABIERTO	
IFX_EITI_COLOMBIA 179.1.211.170 17	SEMANA 3	Oscar Riobamba	EITI-001-17032025	17/03/2025	10:01 PM / 11:08 AM	187	Alta	19/03/2025	ABIERTO	
sith.minminas.gov.co_ifk	SEMANA 3	Jairo Diaz - Jimmy ZEA	SITH-001-17032025	17/03/2025	11:01 PM / 11:12 PM	11	Alta	19/03/2025	ABIERTO	
siveiic_http	SEMANA 3	Oscar Moreno	SIVEEIC-001-17032025	17/03/2025	08:32 AM / 08:40 AM	16	Media	17/03/2025	ABIERTO	
siveiic_https	SEMANA 3	Oscar Moreno	SIVEEIC-001-17032025	17/03/2025	08:32 AM / 08:40 AM	16	Media	17/03/2025	ABIERTO	
siveiic_3020	SEMANA 3	Oscar Moreno	SIVEEIC-001-17032025	17/03/2025	08:32 AM / 08:40 AM	16	Media	17/03/2025	ABIERTO	
siveiic_3010	SEMANA 3	Oscar Moreno	SIVEEIC-001-17032025	17/03/2025	08:32 AM / 08:40 AM	16	Media	17/03/2025	ABIERTO	
VIP_ARGOP	SEMANA 4	Stevens Sandoval - Jenny Nova	ARGOPROD-001-25032025	25/03/2025	10:40 PM / 10:55 PM	15	Alta	26/03/2025	ABIERTO	

Imagen [23]. Seguimiento gestión de vulnerabilidades segundo trimestre.

En la generalidad se presentaron 41 actividades de vulnerabilidades ejecutadas por el equipo de ciberseguridad, esto implica sistemas de información, aplicaciones, servidores e infraestructura interna, se evidencia que dentro de los resultados se tienen 14 situaciones que evidencias vulnerabilidades criticas de las cuales 7 están subsanadas y 7 están en proceso de ejecución,

5.3 PLAN DE AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN

En el marco del cumplimiento del Plan Anual de Auditorías Internas y conforme al cronograma institucional, entre la tercera semana de abril y la primera semana de mayo de 2025 se llevó a cabo una auditoría interna focalizada en el proceso de Gestión Tecnológica, liderada por la Oficina de Planeación y Gestión. Esta actividad tuvo como propósito evaluar la conformidad, eficacia y oportunidad de los controles implementados en materia de seguridad de la información, así como identificar oportunidades de mejora que permitan fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI) y su alineación con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) 2025.

Como resultado de la auditoría, se identificaron dos hallazgos fundamentales que dieron lugar a la formulación de un plan de mejora específico para el proceso evaluado:

Hallazgo 1: Actualización e identificación de activos de información

Se evidenció la necesidad de actualizar el inventario de activos de información conforme a los lineamientos del nuevo MSPI 2025, lo cual incluye el registro integral y clasificado de personas, hardware, software, bases de datos, información, procesos y servicios. El modelo de identificación deberá contemplar las categorías establecidas por el marco normativo para entidades públicas, asegurando su trazabilidad, valoración, relación con servicios institucionales y categorización según impacto en la confidencialidad, integridad y disponibilidad. Para mayor detalle sobre este avance, se recomienda consultar la sección de Activos de Información del presente informe.

Hallazgo 2: Integración de riesgos de seguridad y privacidad con los activos de información

Se estableció que los riesgos de seguridad y privacidad actualmente documentados no se encuentran actualizados ni alineados con el nuevo inventario de activos, lo cual genera una brecha significativa en la gestión de riesgos institucional. La auditoría concluye que, en ausencia de un inventario actualizado, los riesgos permanecen anclados en escenarios y condiciones de ejercicios anteriores, sin reflejar las amenazas emergentes, vulnerabilidades actuales ni cambios tecnológicos recientes. Esta situación limita la efectividad del análisis de riesgos y compromete la toma de

decisiones informadas en materia de mitigación y protección.

A partir de estos hallazgos, se formuló un plan de mejora con acciones específicas, cuyo seguimiento estará a cargo del Grupo de Gestión Tecnológica y de la Oficina Asesora de Planeación. Este plan incluye plazos, responsables y entregables clave orientados a cerrar brechas en la gestión de activos y riesgos, consolidando así una postura institucional más robusta, resiliente y alineada con las exigencias normativas y los desafíos actuales del entorno digital.

6. CAPACITACIÓN Y SENSIBILIZACIÓN

Durante el segundo trimestre de 2025 se impartieron dos sesiones de formación dirigidas a fortalecer la cultura de seguridad digital en la entidad. La primera charla se centró en la gestión de contraseñas seguras, ofreciendo buenas prácticas para su creación, almacenamiento y renovación periódica, así como recomendaciones de herramientas de gestión (password managers) y criterios para definir políticas de longitud y complejidad adaptadas al nivel de riesgo de cada sistema.

La segunda sesión abordó el aprendizaje y la adopción de las políticas de seguridad y privacidad de la información del nuevo Modelo de Seguridad y Privacidad de la Información (MSPI), fundamentadas en la Resolución 40646 de 2023. En ella se explicó el alcance y objetivos de cada política, se discutieron casos prácticos de cumplimiento y sanciones por incumplimiento, y se motivó a los participantes a integrar estos lineamientos en sus rutinas diarias de trabajo.

Simulaciones de ataques: se realizaron ejercicios de simulación de ataques cibernéticos (como campañas de phishing e ingeniería social, resultados en la tabla siguiente) y se proyecta pruebas de hacking ético para detectar brechas de seguridad desde la perspectiva de un atacante, obteniendo hallazgos que permitieron fortalecer la postura de seguridad sin exponer información real.

Tabla-1. Resultados campaña de Pishing cosecha de credenciales junio 2025.

Acción	Numero de colaboradores	Porcentaje
Entregaron credenciales	231	15
Leyeron el mensaje	832	55
Eliminaron el mensaje	376	25
Hicieron clic	351	23

Imagen [24]. Portada capacitación contraseñas seguras.

Imagen [25]. Indice capacitación contraseñas seguras.

Imagen [26]. Portada capacitación políticas de seguridad y privacidad de la información.

Imagen [26]. Sección capacitación políticas de seguridad y privacidad de la información.

Energía