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

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

Elaboró:

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

Andrés Alejandro Ayure
Leidy Paola Galindo Acevedo
Andrés Camilo Molano Mendieta

Entidad:

Ministerio de Minas y Energía

Bogotá, 10 de Abril 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 “Realizar los ajustes y cambios en la metodología de desarrollo en donde se han incorporado los temas de código seguro, actividad 1 :Aplicar el checklist de seguridad definido en la metodología de desarrollo del Ministerio, basado en estándares internacionales como OWASP y PCI DSS.” 12

Riesgo R11 Habilitar y configurar el módulo de auditoría de los SI (aplicaciones, Web Services, Apps, entre otros) acorde con capacidades; actividad 1: Desarrollar y documentar un procedimiento estandarizado para la implementación de módulos de auditoría en todos los sistemas de información críticos del Ministerio. 17

Riesgo R14 Realizar las tareas y actividades de backup, respaldo ydisposición acorde con plan de programación y/o solicitudes puntuales. Actividad 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. 22

Riesgo R21 Falencias en la clasificación de activos de información . Actividad 1 : Identificar y documentar todos los activos de información críticos del Ministerio, asegurando su clasificación de acuerdo con criterios de confidencialidad, integridad y disponibilidad. 26

4.4 GESTIÓN DE POLÍTICAS Y PROCEDIMIENTOS 28

4.5 GESTIÓN DE RECURSOS DE SEGURIDAD 30

5. SEGUIMIENTO PLAN DE ASEGURAMIENTO Y EVALUACIÓN DE LA IMPLEMENTACIÓN Y MANTENIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN 31

5.1 GESTIÓN DE INDICADORES 31

5.2 GESTIÓN DE VULNERABILIDADES. 33

5.3 PLAN DE AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN 38

6. CAPACITACIÓN Y SENSIBILIZACIÓN 38

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. Andrés Alejandro Ayure
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

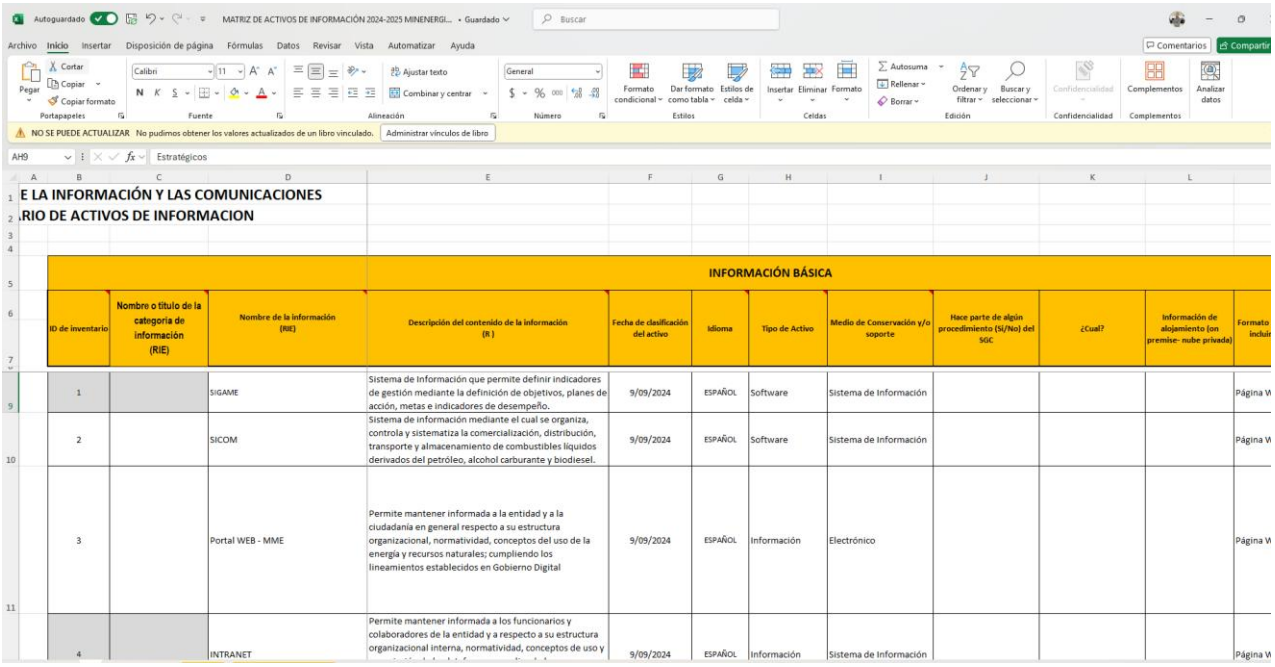
Durante la vigencia 2024, la Gestión de Activos de Información se consolidó como un componente esencial dentro del Plan de Seguridad y Privacidad de la Información del Ministerio de Minas y Energía. Se trazó un cronograma anual para su revisión y actualización, que incluyó la mejora progresiva de la plantilla de inventarios y la categorización de los activos conforme al nuevo mapa de procesos institucionales. Asimismo, se actualizaron las Tablas de Retención Documental (TRD), se elaboró material de apoyo para capacitaciones internas y se implementó un plan piloto con el Grupo TIC que permitió validar una matriz optimizada. Este piloto incorporó criterios de criticidad alineados con las normas ISO/IEC 27001 e ISO/IEC 27005, y se complementó con instrucciones detalladas y un apartado de observaciones que favoreció una evaluación integral de cada activo.

Para la vigencia 2025 en su primer trimestre, se ha dado continuidad a este proceso con una actividad estratégica de alto impacto, orientada a la identificación y documentación de todos los activos de información críticos del Ministerio. Esta actividad fue desarrollada durante el primer trimestre del año en curso mediante una mesa de trabajo interinstitucional que articuló al Grupo de Gestión Documental, la Oficina de Planeación y el Grupo TIC. El objetivo principal fue rediseñar y actualizar la matriz de activos, creando un instrumento unificado, automatizado y funcional que facilite la clasificación bajo los principios de confidencialidad, integridad y disponibilidad (CID), tal como lo exige el marco normativo vigente.

Este nuevo instrumento incorpora elementos del índice de información clasificada y reservada, y se encuentra alineado con los objetivos estratégicos de la entidad. Su diseño permite consolidar la información previamente recolectada por diversas áreas, estandarizando la identificación, valoración y trazabilidad de los activos. Además, se integra con los procesos del Sistema Integrado de Gestión (SIG), lo que refuerza la interoperabilidad institucional, garantiza la eficacia documental, y promueve el cumplimiento normativo. En esta fase inicial de 2025, el instrumento se encuentra en proceso de validación final, pendiente de concertación con las áreas de Comunicaciones y la Oficina Asesora Jurídica (OAJ), tras lo cual se procederá con la socialización y capacitación dirigida a los líderes SIG.

Como parte de la estrategia de automatización y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), se ha iniciado paralelamente el despliegue e integración de la herramienta ERAMBA en la infraestructura tecnológica del Ministerio. Esta plataforma de código abierto está orientada a la gestión de gobierno, riesgos y cumplimiento (GRC), y permitirá llevar un control centralizado, dinámico y escalable del ciclo de vida de los activos de información. A través de

ERAMBA, se sistematizarán procesos como la categorización de activos, análisis de impacto al negocio (BIA), planes de continuidad (BCP), asignación de responsables y seguimiento de controles, alineando la operación institucional con estándares internacionales y fortaleciendo las capacidades institucionales en materia de ciberseguridad, trazabilidad y auditoría.



E LA INFORMACIÓN Y LAS COMUNICACIONES
RIO DE ACTIVOS DE INFORMACION

				INFORMACIÓN BÁSICA								
ID de inventario	Nombre o título de la categoría de información (RIE)	Nombre de la información (RIE)	Descripción del contenido de la información (R)	Fecha de clasificación del activo	Idioma	Tipo de Activo	Medio de Conservación y/o soporte	Hace parte de algún procedimiento (SI/No) del SGC	¿Cual?	Información de alojamiento (on premise- nube privada)	Formato incluir
1		SIGAME	Sistema de Información que permite definir indicadores de gestión mediante la definición de objetivos, planes de acción, metas e indicadores de desempeño.	9/09/2024	ESPAÑOL	Software	Sistema de Información				Página W
2		SICOM	Sistema de información mediante el cual se organiza, controla y sistematiza la comercialización, distribución, transporte y almacenamiento de combustibles líquidos derivados del petróleo, alcohol carburante y biodiesel.	9/09/2024	ESPAÑOL	Software	Sistema de Información				Página W
3		Portal WEB - MME	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	9/09/2024	ESPAÑOL	Información	Electrónico				Página W
4		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	9/09/2024	ESPAÑOL	Información	Sistema de Información				Página W

Imagen [1]. integración de nuevos índices dentro del instrumento de Matriz de activos de información.

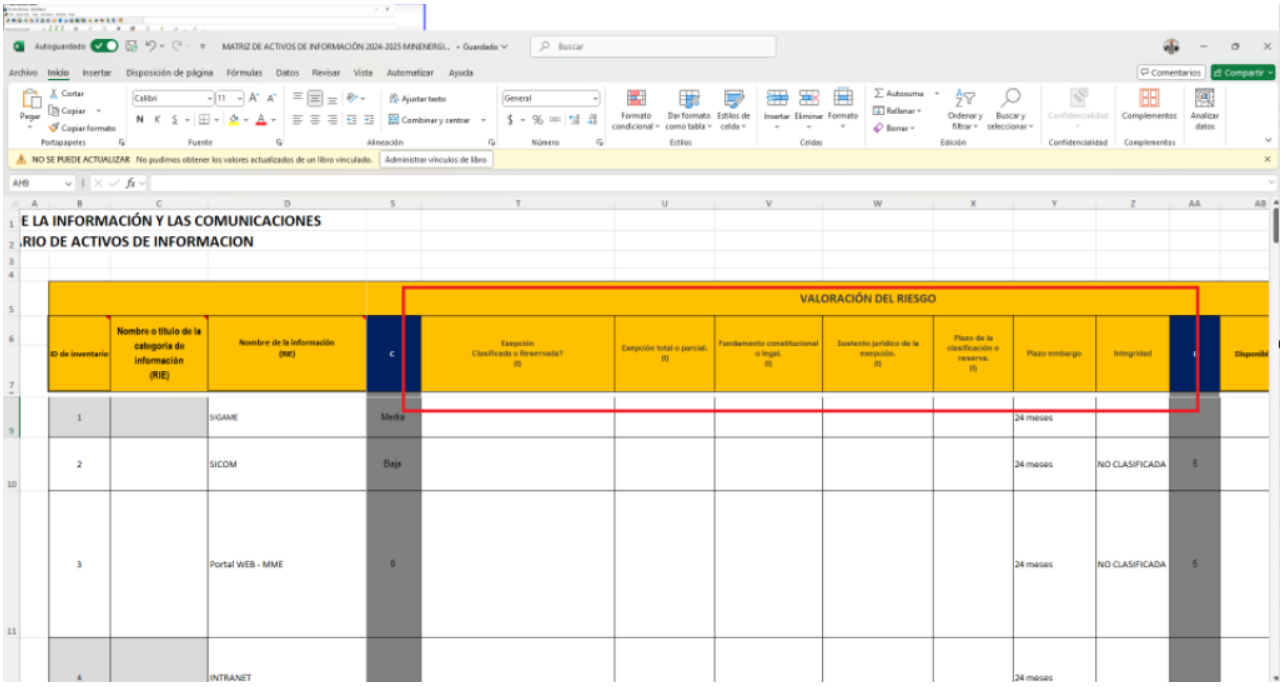


Imagen [2]. integración de nuevos índices dentro del instrumento de Matriz de activos de información.

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	Tercera semana – Mayo 2025	Cuarta semana – Mayo 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 - Junio 2025	Tercera semana - Junio 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 - Junio 2025	Cuarta semana - Junio 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 - Junio 2025	Primera Semana - Julio 2025	En caso de presentarse información faltante o incompleta generar retroalimentación.
Entrega de información ajustada	Responsables de cada dependencia	Segunda Semana - Julio 2025	Cuarta semana - Julio2025	Información debidamente ajustada y completada.
Validación y priorización de activos críticos	Oficial de Seguridad o quien haga sus veces	Primera semana - Agosto 2025	Segunda semana - Agosto 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	Agosto 2025	Agosto 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	Gestion	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						TODOS LOS PROCESOS		
							Evaluación del riesgo - Valoración de los controles		
%	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 metodología de desarrollo del ministerio, basado en estándares internacionales como OWASP y PCI DSS, adicionalmente, programa auditorías trimestrales en los sistemas de información para evaluar la correcta implementación de los lineamientos de código seguro, si encuentra inconsistencias en la auditoría 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 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.

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

2	GESTIÓN TECNOLÓGICA	Gestion	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 auditoría, 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 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.

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 critica 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 critica 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.

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).

5	GESTIÓN TECNOLÓGICA	Gestión	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.

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 "Realizar los ajustes y cambios en la metodología de desarrollo en donde se han incorporado los temas de código seguro, actividad 1 :Aplicar el checklist de seguridad definido en la metodología de desarrollo del Ministerio, basado en estándares internacionales como OWASP y PCI DSS."

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 3.
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.

Para el primer trimestre se anexa el uso de los diferentes lenguajes de programación que maneja el equipo de desarrollo y sobre que sistemas de información (remitirse al Equipo de Desarrollo del Grupo TICS para saber acerca de estos activos de información), y software quese encuentran actualmente. Además, se determinan las preguntas objeto de "check list" para poder determinar la Hoja de Ruta del Desarrollo Seguro.

- **Python:** Es un lenguaje de alto nivel de programación y es muy pragmático en la legibilidad de su código, se utiliza para desarrollar aplicaciones de todo tipo, web, local, hibrido, entre otros.

- **Java:** Permite escribir, compilar, depurar diferentes funcionalidades orientado a objetos de los sistemas de información.

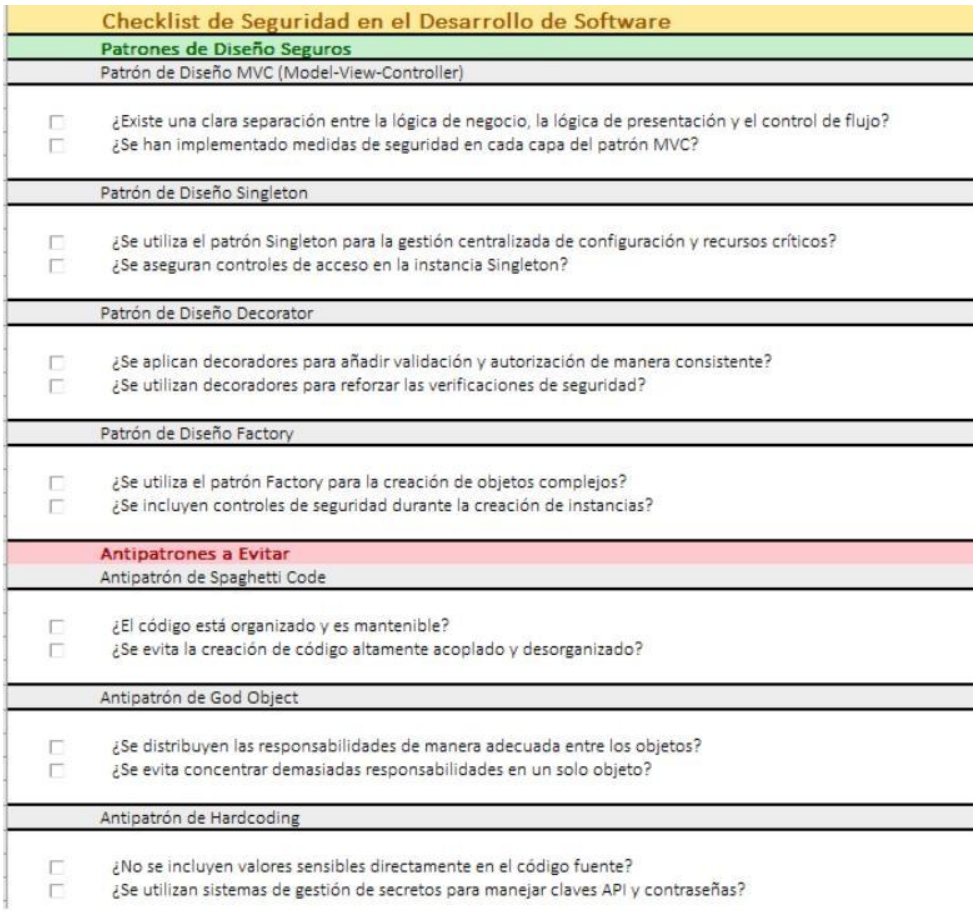
- **Java Script:** Es un lenguaje de programación que es similar a Java teniendo en cuenta que estos mismos están orientado a objetos lo que permite que tenga mayor manejo en la interpretación y el dialecto en los prototipos.

- **CSS:** Es un lenguaje que abarca toda la estructura de diseño visual y/o gráfico y se enfoca en desarrollo web.

- **HTML 5:** Permite crear la estructura de páginas web, donde se incorporan posteriormente imágenes, textos, vídeos y todo tipo de material multimedia de forma que se pueda visualizar correctamente.

- **SQL:** El lenguaje de consulta estructurada (SQL) es un lenguaje de consulta popular que se usa con frecuencia en todos los tipos de aplicaciones. Analistas y desarrolladores de datos aprenden y usan SQL porque se integra bien con los diferentes lenguajes de programación.

- **.NET:** Es una plataforma de código abierto que permite crear aplicaciones locales,web y móviles que se pueden ejecutar de forma nativa en cualquier sistema operativo.Este mismo incluye herramientas, bibliotecas y lenguajes que admiten el desarrollo de software moderno, escalable y de alto rendimiento.



Checklist de Seguridad en el Desarrollo de Software	
Patrones de Diseño Seguros	
Patrón de Diseño MVC (Model-View-Controller)	
☐	¿Existe una clara separación entre la lógica de negocio, la lógica de presentación y el control de flujo?
☐	¿Se han implementado medidas de seguridad en cada capa del patrón MVC?
Patrón de Diseño Singleton	
☐	¿Se utiliza el patrón Singleton para la gestión centralizada de configuración y recursos críticos?
☐	¿Se aseguran controles de acceso en la instancia Singleton?
Patrón de Diseño Decorator	
☐	¿Se aplican decoradores para añadir validación y autorización de manera consistente?
☐	¿Se utilizan decoradores para reforzar las verificaciones de seguridad?
Patrón de Diseño Factory	
☐	¿Se utiliza el patrón Factory para la creación de objetos complejos?
☐	¿Se incluyen controles de seguridad durante la creación de instancias?
Antipatrones a Evitar	
Antipatrón de Spaghetti Code	
☐	¿El código está organizado y es mantenible?
☐	¿Se evita la creación de código altamente acoplado y desorganizado?
Antipatrón de God Object	
☐	¿Se distribuyen las responsabilidades de manera adecuada entre los objetos?
☐	¿Se evita concentrar demasiadas responsabilidades en un solo objeto?
Antipatrón de Hardcoding	
☐	¿No se incluyen valores sensibles directamente en el código fuente?
☐	¿Se utilizan sistemas de gestión de secretos para manejar claves API y contraseñas?

Imagen [11]. Preguntas de seguridad para el desarrollo de software y las buenas prácticas -base 1.

	Antipatrón de Copy-Paste Programming
☐	¿Se evita la duplicación de código?
☐	¿Se mantiene la consistencia y se facilita la actualización del código?
	Arquitecturas Seguras
	Arquitectura de Microservicios
☐	¿Los servicios están aislados y se comunican a través de APIs?
☐	¿Se gestionan autenticación y autorización de manera centralizada mediante un gateway de API?
	Arquitectura en Capas (Layered Architecture)
☐	¿Se implementan múltiples capas de seguridad en la arquitectura?
☐	¿Cada capa añade redundancia y control de seguridad?
	Arquitectura Event-Driven
☐	¿Se utilizan colas de mensajes y brokers seguros para la comunicación entre componentes?
☐	¿Se asegura la integridad y confidencialidad de los datos en tránsito?
	Arquitectura Zero Trust
☐	¿Se verifica continuamente cada solicitud y acceso a recursos?
☐	¿No se asume confianza implícita dentro de la red?
	Prácticas de Desarrollo Seguro
	Principio de Privilegio Mínimo
☐	¿Cada componente del sistema y usuario tiene solo los permisos necesarios?
☐	¿Se revisan y ajustan regularmente los permisos para reducir la superficie de ataque?
	Ciclo de Vida de Desarrollo Seguro (SDLC)
☐	¿Se integran evaluaciones y pruebas de seguridad desde la planificación hasta el despliegue y mantenimiento?
☐	¿Se realizan revisiones de seguridad en cada fase del desarrollo?

Imagen [12]. Preguntas de seguridad para el desarrollo de software y las buenas prácticas -base 2.

	Definición de Controles de Seguridad en el Código
☐	¿Se utilizan listas blancas para validar entradas y listas negras para bloquear entradas peligrosas conocidas?
☐	¿Se asegura que los datos sensibles estén cifrados tanto en tránsito como en reposo?
	Revisiones de Código y Pruebas
☐	¿Se implementan revisiones de código por pares enfocadas en identificar vulnerabilidades de seguridad?
☐	¿Se integran herramientas de análisis estático (SAST) y dinámico (DAST) en el flujo de trabajo de CI/CD?
	Monitoreo y Respuesta a Incidentes
	Monitorización y Registro Avanzado
☐	¿Se mantiene un registro detallado de las actividades de los usuarios?
☐	¿Se configuran alertas en tiempo real para actividades sospechosas?
	Protección contra Exfiltración de Datos
☐	¿Se implementan soluciones DLP para monitorear y proteger la información sensible?
☐	¿Se aseguran todas las comunicaciones internas entre servicios?
	Seguridad en la Infraestructura
	Seguridad en la Nube
☐	¿Se implementan controles de seguridad específicos para entornos en la nube?
☐	¿Se configuran firewalls y sistemas de detección de intrusos (IDS/IPS)?
	Seguridad de Red
☐	¿Se configura la seguridad de red adecuada para prevenir accesos no autorizados?
☐	¿Se utilizan técnicas de microsegmentación para limitar el movimiento lateral?

Imagen [13]. Preguntas de seguridad para el desarrollo de software y las buenas prácticas -base 3

El informe correspondiente a marzo 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 críticos como AVANZAME y el sistema de gestión de correos. Este enfoque busca prevenir situaciones de conflicto de interés o manipulación indebida de soluciones TIC, manteniendo altos estándares de seguridad y transparencia.

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. 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 documento o al líder del equipo de Desarrollo del Grupo TICS.

Riesgo R11 Habilitar y configurar el módulo de auditoría de los SI (aplicaciones, Web Services, Apps, entre otros) acorde con capacidades; actividad 1: Desarrollar y documentar un procedimiento estandarizado para la implementación de módulos de auditoría en todos los sistemas de información críticos del Ministerio.

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”.

Para el informe del primer 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 [14]. Hoja de ruta para procesos de auditoria en los SI.

Teniendo en cuenta lo anterior, se tiene en la actualidad 13 sistemas de información con módulo de auditoria (a continuación, se muestran algunos ejemplos del proceso 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 [15]. Ejemplo de auditoria SI SISEG, listado de acceso por usuarios (los usuarios expuestos son casos de ejemplo no correspondiente a credenciales reales).

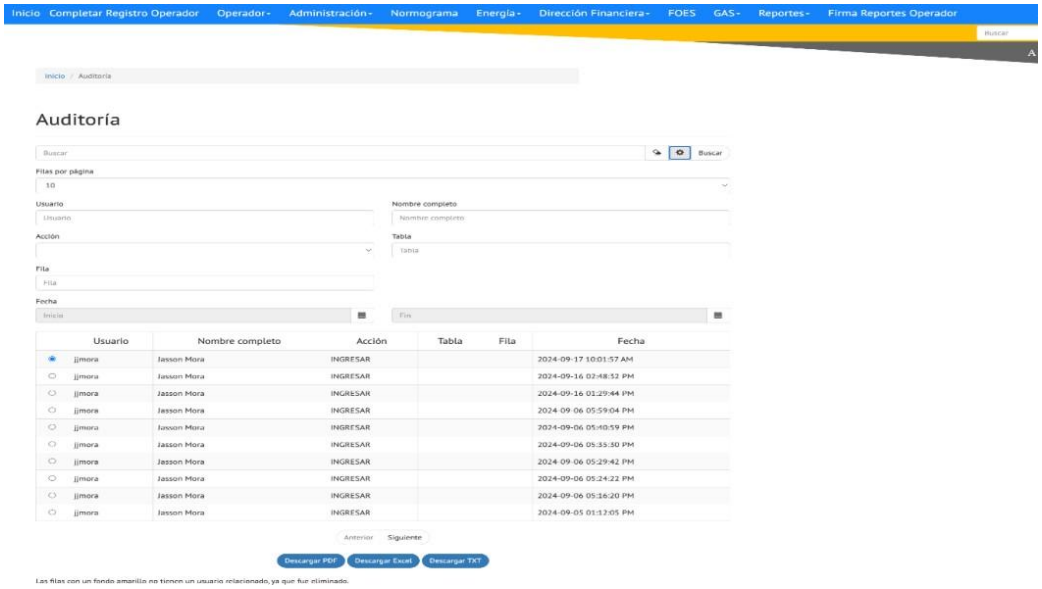


Imagen [16]. Ejemplo de auditoria SI SISEG, filtrado (los usuarios expuestos son casos de ejemplo)

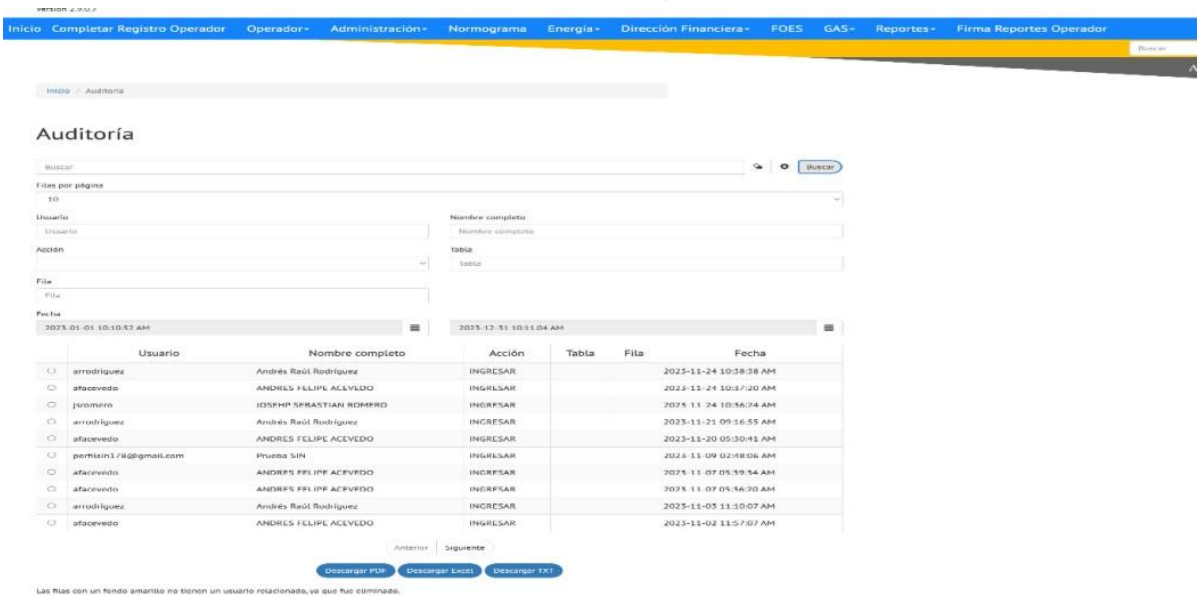


Imagen [17]. Ejemplo de auditoria SI SISEG, años anteriores (los usuarios expuestos son casos de ejemplo no correspondiente a credenciales reales).

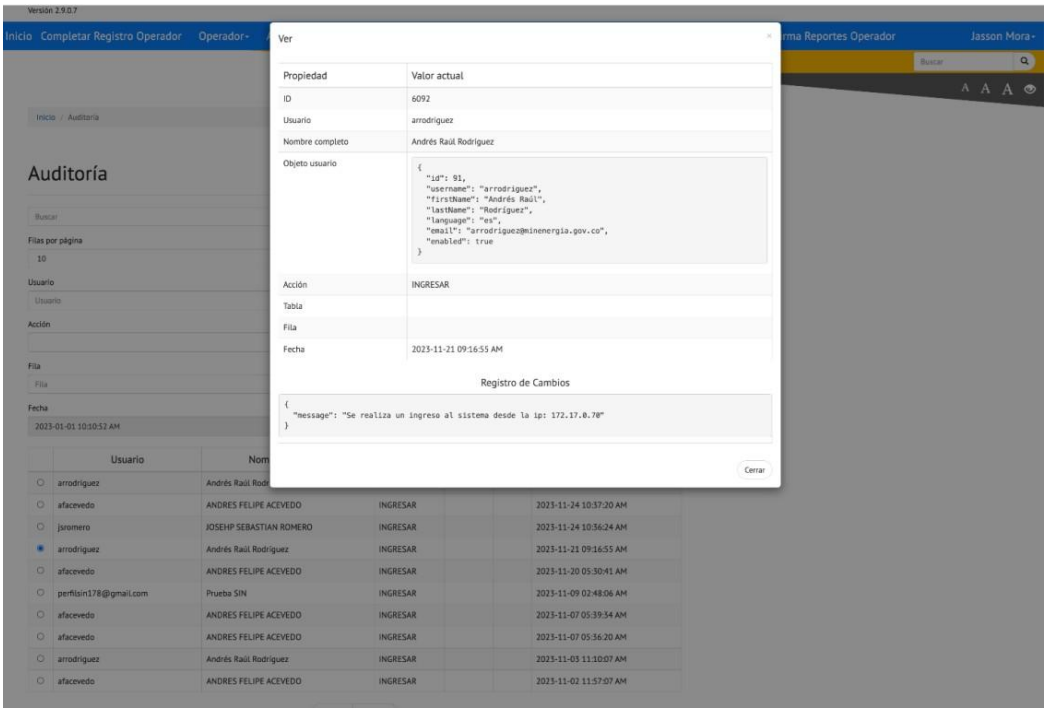


Imagen [18]. Ejemplo de auditoria SI SISEG, detalle de movimientos (los usuarios expuestosson casos de ejemplo no correspondiente a credenciales reales).

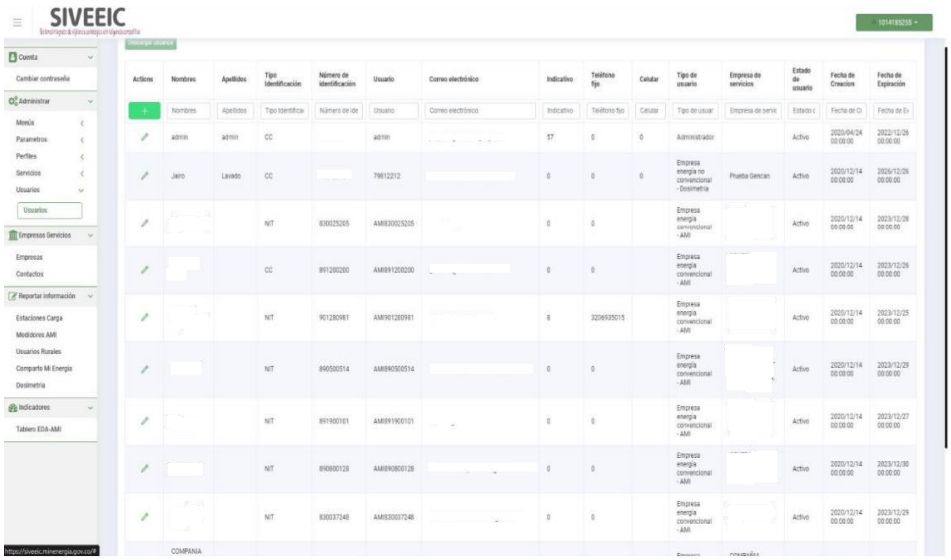


Imagen [19]. Ejemplo de auditoria SI SIVEEIC, detalle de movimientos.

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.

Dicho lo anterior se muestran a continuación dos ejemplos de auditoría realizados condicha herramienta:

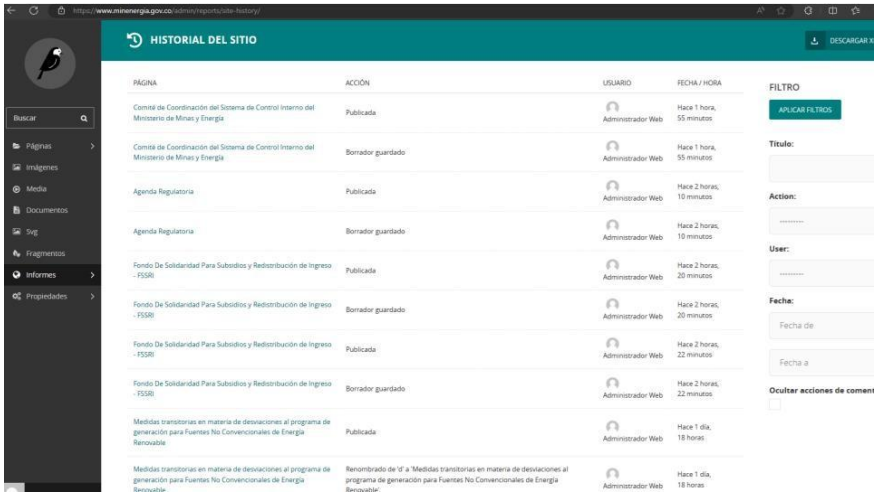


Imagen [20]. Ejemplo de auditoria SI PORTAL WEB, detalle de movimientos.

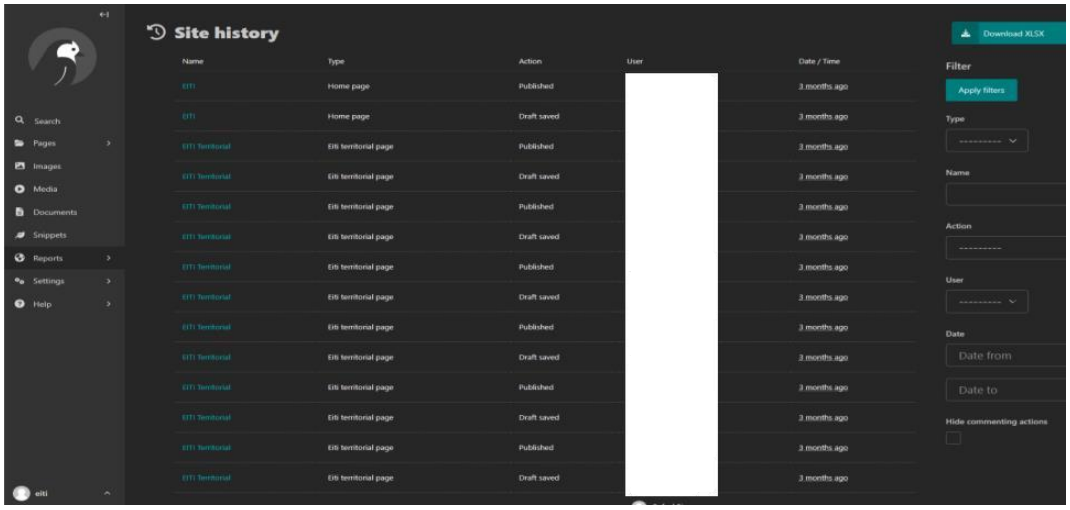


Imagen [21]. Ejemplo de auditoria SI EITI Colombia, detalle de movimientos.

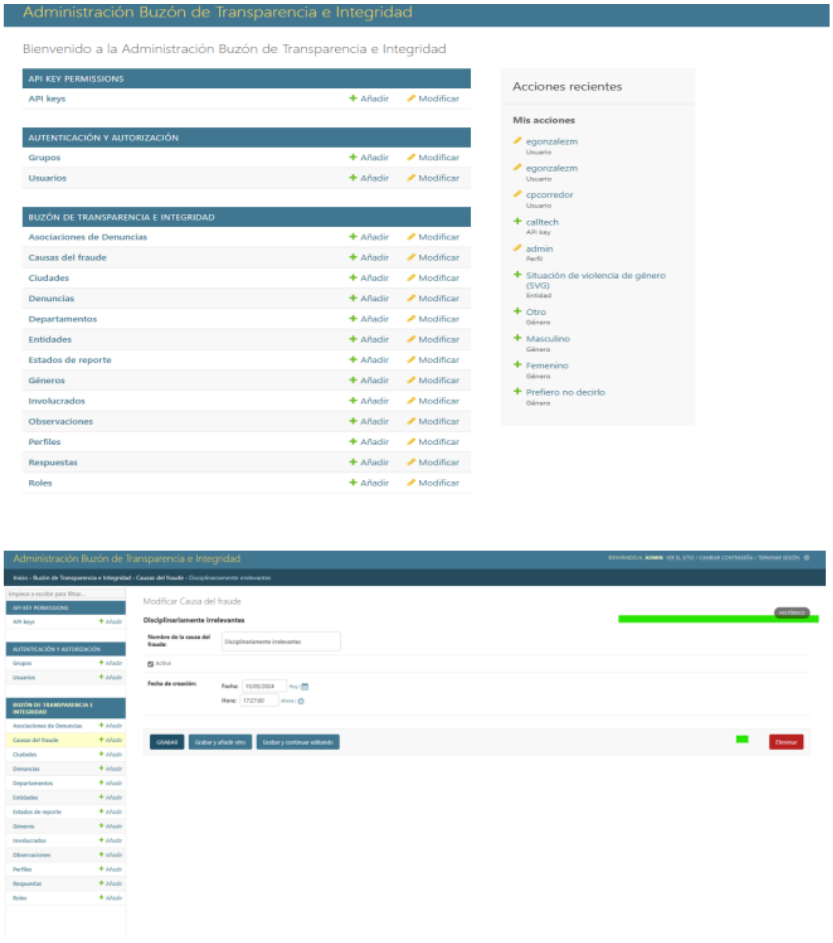


Imagen [22]. Ejemplo de auditoria Buzón de integridad y transparencia.

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.

Adicionalmente, se cuenta dentro de los activos de información del Ministerio de Minasy Energía los aplicativos móviles que también poseen módulos de auditoría, a continuación, se muestra los ítems que contiene y los resultados públicos que se pueden establecer, si se desea más información de datos que pueda proveer consultarcon el encargado de seguridad de la información o el Equipo de Desarrollo del grupo TICS.

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

El proceso de gestión y monitoreo de los respaldos es esencial para asegurar la disponibilidad y la integridad de los datos de la infraestructura tecnológica de la organización. En este contexto, se han llevado a cabo varias actividades durante el primer trimestre para mitigar riesgos asociados con la saturación del sistema y mejorar la eficiencia operativa de la herramienta Arcserve ASBU y UDP Backup. A través de la implementación de métricas clave, se ha buscado garantizar que el sistema de respaldo se mantenga en niveles óptimos de rendimiento, sin llegar a un punto de saturación que comprometa su eficacia.

La actividad realizada ha estado enfocada en dos aspectos fundamentales: por un lado, se ha logrado consolidar el respaldo de servidores críticos, y por otro, se han llevado a cabo tareas de depuración y optimización del espacio de almacenamiento, lo que ha permitido no solo mejorar el rendimiento general del sistema de respaldos, sino también asegurar que el mismo esté alineado con los estándares requeridos para mantener la continuidad del negocio. A continuación, se detallan las actividades específicas realizadas, los resultados alcanzados y las medidas adoptadas para evaluar la continuidad de la herramienta en el futuro.

Detalle de actividades realizadas

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

Durante el primer trimestre, se logró consolidar la herramienta Arcserve UDP Backup, que ha sido implementada como solución principal de respaldo en la infraestructura tecnológica de la organización. En total, se han respaldado XXX servidores críticos, garantizando la protección de datos importantes y la capacidad de recuperación en caso de incidentes. Esta consolidación se ha realizado de manera progresiva, asegurando que cada servidor sea respaldado correctamente y que los tiempos de recuperación se mantengan dentro de los estándares esperados.

La estrategia de respaldo ha sido diseñada para reducir el impacto en el rendimiento del sistema, al tiempo que proporciona una cobertura completa para todos los servidores relevantes. La configuración de la herramienta ha sido afinada en función de las necesidades específicas de la infraestructura tecnológica, logrando optimizar tanto los tiempos de respaldo como los tiempos de recuperación, factores clave en la mitigación de riesgos.

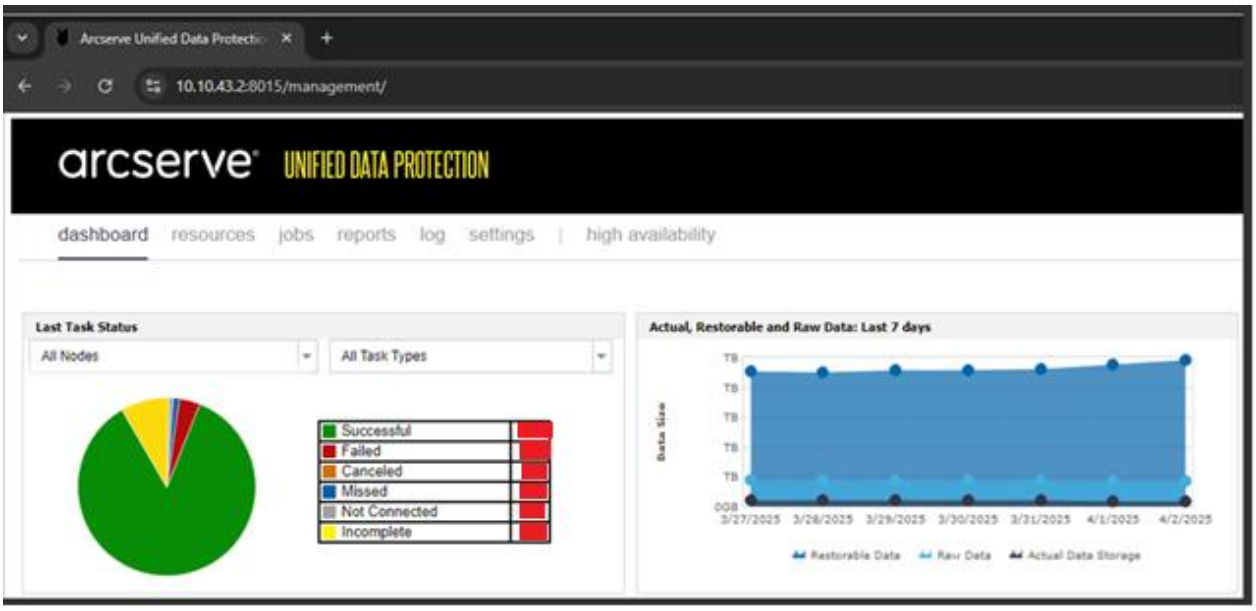


Imagen [23]. Interfaz de proceso de respaldo de los servidores, proceso fallidos, cancelados y satisfactorios.

2. **Depuración de los puntos de restauración históricos con el proveedor SVAIT**

Paralelamente a la consolidación de la herramienta de respaldo, se ha trabajado de manera colaborativa con el proveedor SVAIT en la depuración de los puntos de restauración históricos. Esta

actividad ha sido esencial para liberar espacio de almacenamiento y garantizar que solo los puntos de restauración necesarios y actuales sean conservados. La depuración de estos puntos ha sido un proceso meticuloso que ha permitido reducir el volumen de datos innecesarios almacenados en el sistema.

Gracias a esta depuración, se han eliminado 20TB de datos, lo que ha permitido liberar espacio crítico en la partición x:\XXXXataX. Antes de esta actividad, el espacio disponible era de X.5TB, lo que limitaba la capacidad de almacenamiento y afectaba la eficiencia del sistema de respaldo.

Al liberar estos 20TB adicionales, el espacio total disponible pasó de XX.5TB a XX.5TB, lo que representa un aumento significativo en la capacidad de almacenamiento. Este espacio adicional no solo mejora la capacidad operativa de la herramienta de respaldo, sino que también reduce el riesgo de saturación y mejora el rendimiento general del sistema.

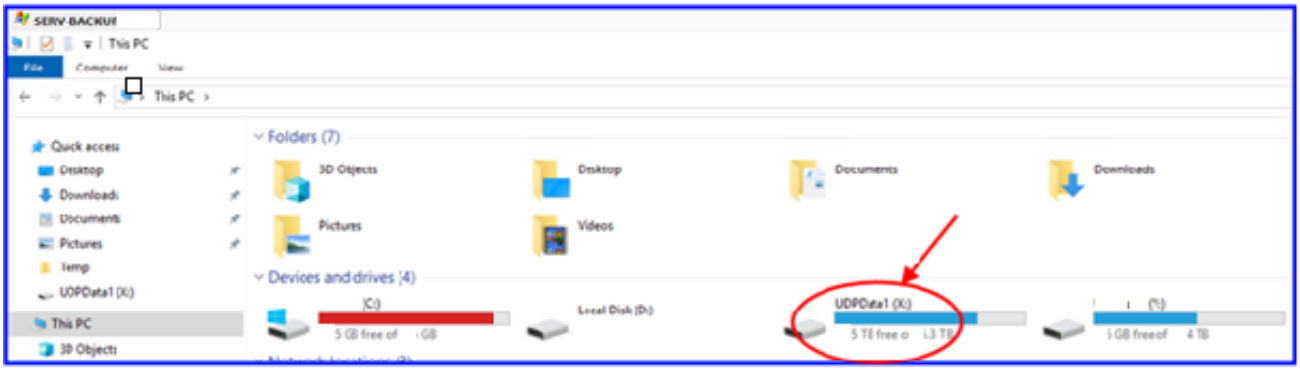


Imagen [24]. Evidencia de liberación de espacio gracias a la depuración de puntos e restauración históricos.

3. Relanzamiento de los backups de Correos y bases de datos

La liberación de espacio mediante la depuración de los puntos de restauración históricos ha tenido un impacto directo en el relanzamiento de los backups de correos electrónicos y bases de datos, que se encontraban represados debido a la falta de espacio. Esta situación había generado un retraso en los respaldos de datos críticos, lo que representaba un riesgo importante en términos de disponibilidad y recuperación.

Una vez que el espacio fue liberado, se pudieron reanudar los procesos de respaldo de correos y bases de datos de manera inmediata. Estos datos son fundamentales para el negocio, ya que incluyen información clave relacionada con las comunicaciones internas y las transacciones comerciales. Al relanzar estos backups, se ha asegurado que todos los datos se encuentren protegidos y disponibles para su recuperación en caso de ser necesario.

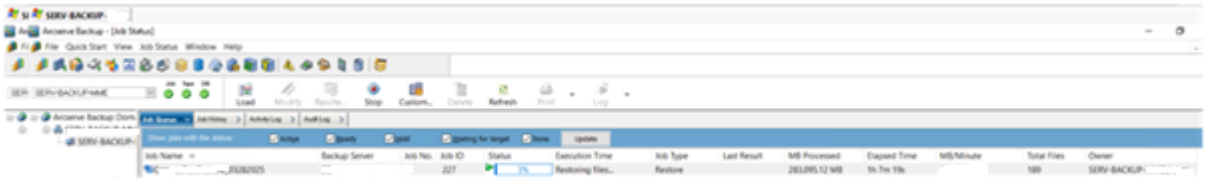


Imagen [25]. Evidencia de impacto sobre los respaldos de correos y bases de datos.

4. **Planificación y ejecución del Backup Full granular a cinta para el mes de marzo de 2025**

Como parte de la estrategia a largo plazo, una vez concluida la labor de depuración de los puntos de restauración históricos, se tiene previsto lanzar un Backup Full Granular a Cinta correspondiente al mes de marzo de 2025. Este tipo de respaldo proporciona una capa adicional de seguridad al permitir la creación de copias de seguridad físicas, las cuales se almacenarán en cintas, un medio de almacenamiento que ha demostrado ser confiable para la conservación de grandes volúmenes de datos a largo plazo.

La implementación de este respaldo completo granular a cinta también servirá para complementar los respaldos realizados a disco, proporcionando una solución de almacenamiento redundante que aumente la resiliencia del sistema frente a cualquier tipo de eventualidad o fallo. Este proceso se llevará a cabo en un entorno controlado, donde se garantice que los tiempos de recuperación sean los adecuados y que se puedan restaurar los datos de manera eficiente si fuera necesario.

Evaluación y futuro de la herramienta de respaldo

A medida que avanzan estas actividades, se implementarán las métricas clave que permitirán evaluar el desempeño de la herramienta Arcserve ASBU y UDP Backup. Estas métricas incluirán:

1. **Tasas de éxito/falla:** Para monitorear la efectividad de los procesos de respaldo y restauración.
2. **Capacidad de almacenamiento disponible:** Para verificar que el sistema de respaldo no esté alcanzando límites críticos de almacenamiento.
3. **Tiempos de recuperación:** Para asegurar que los datos puedan ser recuperados de manera rápida y eficiente en caso de un desastre o pérdida de datos.

Estas métricas no solo permitirán medir la efectividad de las actividades implementadas hasta el momento, sino también determinar si la herramienta Arcserve es la más adecuada para continuar brindando un respaldo confiable. En caso de que las métricas no alcancen los estándares requeridos, se explorarán alternativas que garanticen un rendimiento óptimo y alineado con las necesidades de la organización.

Conclusión

En resumen, las actividades realizadas en este primer trimestre han sido fundamentales para mejorar la eficiencia y la capacidad operativa del sistema de respaldos de la organización. Gracias a la consolidación de la herramienta Arcserve UDP Backup, la depuración de los puntos de restauración históricos y el relanzamiento de los backups de correos y bases de datos, se ha logrado una optimización significativa del espacio de almacenamiento y una mejora en los tiempos de recuperación. La planificación del Backup Full Granular a Cinta para marzo de 2025 refuerza aún más la estrategia de recuperación ante desastres, asegurando una solución de respaldo robusta y confiable. Con la implementación de métricas clave, se podrá evaluar de manera precisa el desempeño del sistema y tomar decisiones informadas sobre la continuidad o posible reemplazo de la herramienta de respaldo.

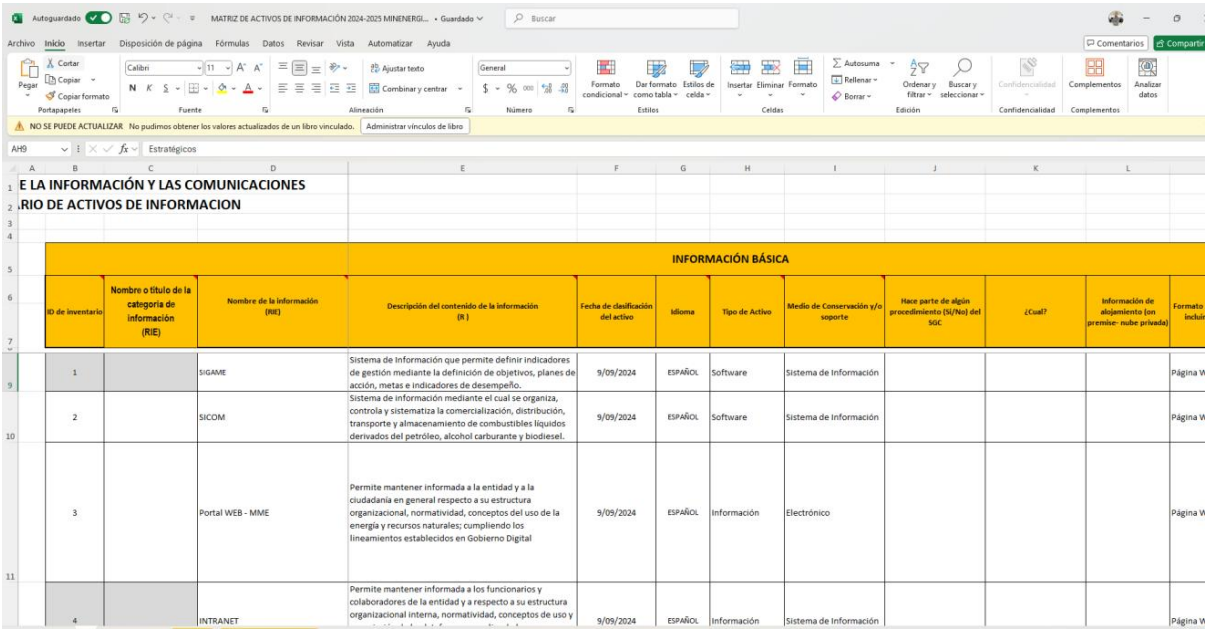
Riesgo R21 Falencias en la clasificación de activos de información . Actividad 1 : Identificar y documentar todos los activos de información críticos del Ministerio, asegurando su clasificación de acuerdo con criterios de confidencialidad, integridad y disponibilidad.

En seguimiento al tratamiento del riesgo R21 primer trimestre, identificado como “Falencias en la clasificación de activos de información”, se desarrolló una actividad estratégica orientada a la identificación y documentación de todos los activos de información críticos del Ministerio de Minas y Energía. Esta tarea se abordó con un enfoque integral y colaborativo, mediante la realización de una mesa de trabajo interinstitucional que reunió al Grupo de Gestión Documental, la Oficina de Planeación y el Grupo TIC. El objetivo central fue redefinir y modificar la matriz de activos de información existente, con el fin de consolidar un instrumento unificado, automatizado y funcional para todas las áreas de la entidad. Este esfuerzo busca facilitar la clasificación de activos bajo los criterios de confidencialidad, integridad y disponibilidad, garantizando así una base sólida para la gestión de riesgos de seguridad de la información.

Durante el proceso, se avanzó significativamente en la finalización técnica del nuevo instrumento, el cual incorpora elementos del índice de información clasificada y reservada, alineándolos con los objetivos estratégicos institucionales. Este instrumento, además de unificar la información previamente diligenciada por diversas áreas, permitirá estandarizar la forma en que se identifican y valoran los activos de información. La herramienta también facilitará su interoperabilidad con otros procesos clave del Sistema Integrado de Gestión (SIG), lo que redundará en una mayor eficiencia, trazabilidad y cumplimiento normativo en la gestión de activos.

Actualmente, el instrumento se encuentra en su fase final de validación, pendiente de una reunión con las áreas de Comunicaciones y la Oficina Asesora Jurídica (OAJ). Posteriormente, se dará inicio a un proceso de capacitación dirigido a los líderes del SIG, quienes tendrán un rol protagónico en el despliegue e implementación de la herramienta. A partir de este ejercicio, se proyecta la actualización adecuada de los análisis de impacto al negocio (BIA) y de los planes de continuidad del negocio

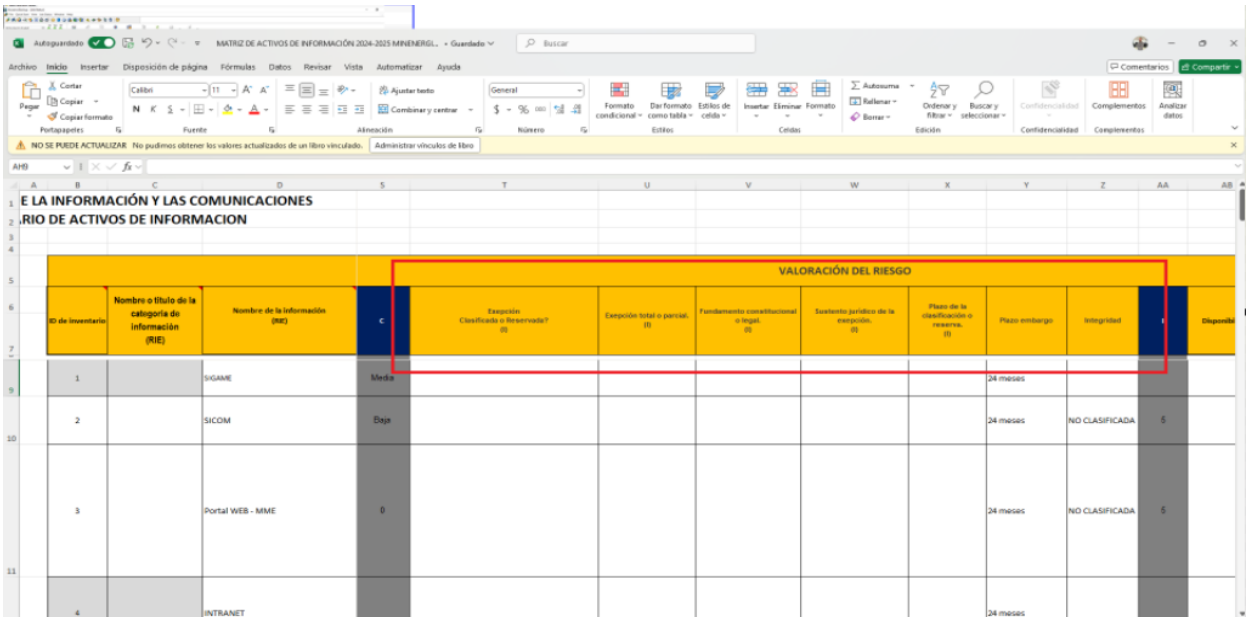
(BCP), fortaleciendo así la preparación institucional ante eventos que puedan comprometer la disponibilidad o integridad de la información crítica, en concordancia con las exigencias del marco de seguridad de la información y continuidad operativa.



E LA INFORMACIÓN Y LAS COMUNICACIONES
RIO DE ACTIVOS DE INFORMACION

			INFORMACIÓN BÁSICA									
ID de inventario	Nombre o título de la categoría de información (RIE)	Nombre de la información (RIE)	Descripción del contenido de la información (R)	Fecha de clasificación del activo	Idioma	Tipo de Activo	Medio de Conservación y/o soporte	Hace parte de algún procedimiento (Si/No) del SGC	¿Cual?	Información de alojamiento (on premise- nube privada)	Formato incluir
1		SIGAME	Sistema de Información que permite definir indicadores de gestión mediante la definición de objetivos, planes de acción, metas e indicadores de desempeño.	9/09/2024	ESPAÑOL	Software	Sistema de Información				Página W
2		SICOM	Sistema de información mediante el cual se organiza, controla y sistematiza la comercialización, distribución, transporte y almacenamiento de combustibles líquidos derivados del petróleo, alcohol carburante y biodiesel.	9/09/2024	ESPAÑOL	Software	Sistema de Información				Página W
3		Portal WEB - MME	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	9/09/2024	ESPAÑOL	Información	Electrónico				Página W
4		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	9/09/2024	ESPAÑOL	Información	Sistema de Información				Página W

Imagen [25]. integración de nuevos índices dentro del instrumento de Matriz de activos de información.



E LA INFORMACIÓN Y LAS COMUNICACIONES
RIO DE ACTIVOS DE INFORMACION

				VALORACIÓN DEL RIESGO								
ID de inventario	Nombre o título de la categoría de información (RIE)	Nombre de la información (RIE)	C	Excepción Clasificada o Reservada? (I)	Excepción total o parcial. (I)	Fundamento constitucional o legal. (I)	Sustento jurídico de la excepción. (I)	Plazo de la clasificación o reserva. (I)	Plazo embargo	Integridad	I	Disponibi
1		SIGAME	Media						24 meses			
2		SICOM	Baja						24 meses	NO CLASIFICADA	5	
3		Portal WEB - MME	0						24 meses	NO CLASIFICADA	5	
4		INTRANET							24 meses			

Imagen [18]. integración de nuevos índices dentro del instrumento de Matriz de activos de información.

4.4 GESTIÓN DE POLÍTICAS Y PROCEDIMIENTOS

Para el primer trimestre del 2025, se tuvo un mesa de trabajo conforme a los requerimientos del En el marco del proceso de estandarización de la Arquitectura Empresarial (AE) del proceso de gestión tecnológica del Ministerio de Minas y Energía, se continúa avanzando en la articulación de los componentes estratégicos, normativos y operativos que integran el Modelo Integrado de Planeación y Gestión (MIPG), los lineamientos de la Política de Confianza y Seguridad Digital, la Resolución 40646 de la entidad, y el Sistema de Gestión de Seguridad de la Información (SGSI). En este contexto, se encuentran en fase de revisión y aprobación dos documentos clave: el Procedimiento de Monitoreo y Gestión de Incidentes de Seguridad de la Información, y la Política de Privacidad para el Tratamiento de Datos Personales del sistema SICOM. Ambos instrumentos responden a la necesidad de robustecer el marco de actuación ante incidentes y riesgos asociados a la protección de la información institucional y de los datos personales tratados en dicho sistema.

Este proceso se ha desarrollado bajo un enfoque de mejora continua, con retroalimentación activa por parte de la Oficina de Planeación y Gestión Internacional, especialmente en su fase final, donde se han propuesto ajustes para optimizar los procedimientos y flujos definidos. En lo que respecta a la política de tratamiento de datos personales, se ha definido que esta hará referencia a la política vigente del Ministerio de Minas y Energía, respetando así su marco normativo institucional. No obstante, para dar cumplimiento a los requerimientos específicos de SICOM, se ha solicitado la elaboración de un manual complementario que detalle los aspectos operativos y técnicos exigidos por el sistema, en armonía con las disposiciones de la Ley 1581 de 2012 y el Decreto 1377 de 2013.

De manera paralela, se han identificado nuevos requerimientos normativos y técnicos que serán abordados a partir del segundo trimestre de 2025. Entre ellos se encuentran: la elaboración de una Política de Uso Responsable de Inteligencia Artificial, que establecerá principios éticos, técnicos y de control aplicables a soluciones basadas en IA dentro de la entidad; el diseño de la Política de Ciclo de Vida del Hardware Obsoleto, que establecerá directrices claras sobre la disposición, reutilización o destrucción segura de equipos fuera de operación en los centros de datos (como switches, servidores, entre otros); y la revisión de los Acuerdos de Confidencialidad vigentes entre SICOM y proveedores externos, en especial aquellos relacionados con la ejecución de pruebas de penetración (pentesting), para asegurar el cumplimiento de estándares de privacidad, no divulgación y tratamiento seguro de vulnerabilidades.

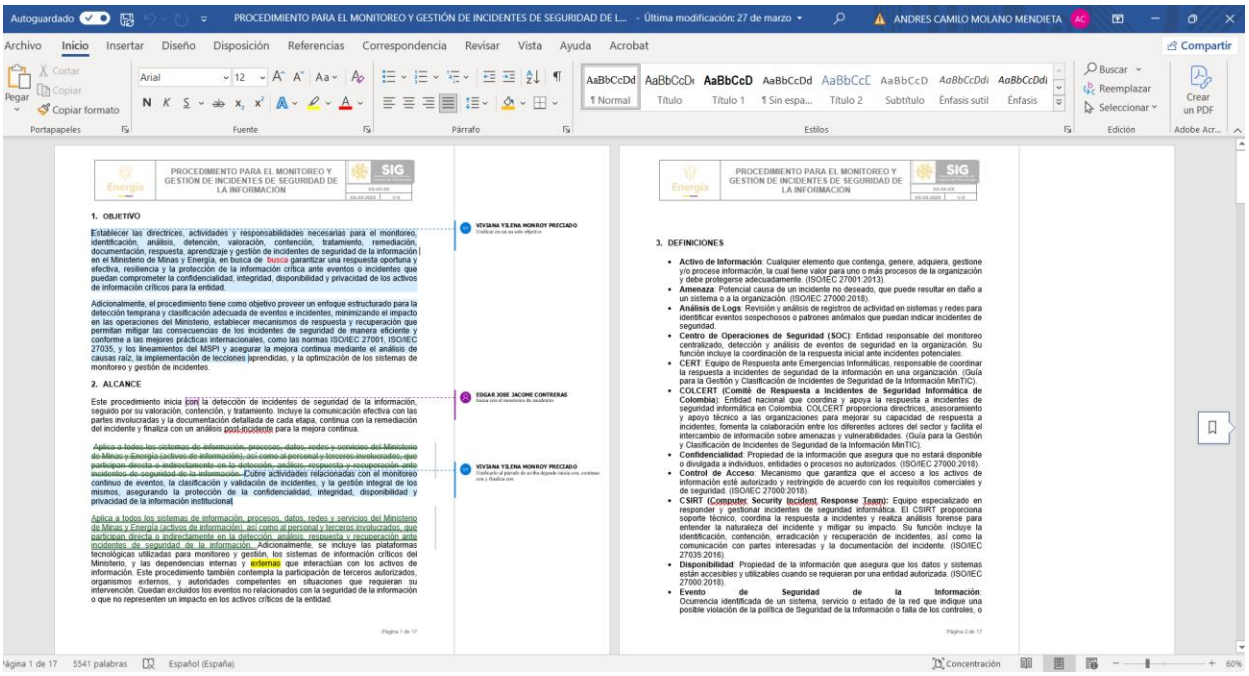


Imagen [19]. Control de cambios y observaciones del procedimiento de monitoreo y gestión de incidentes de seguridad de la información.

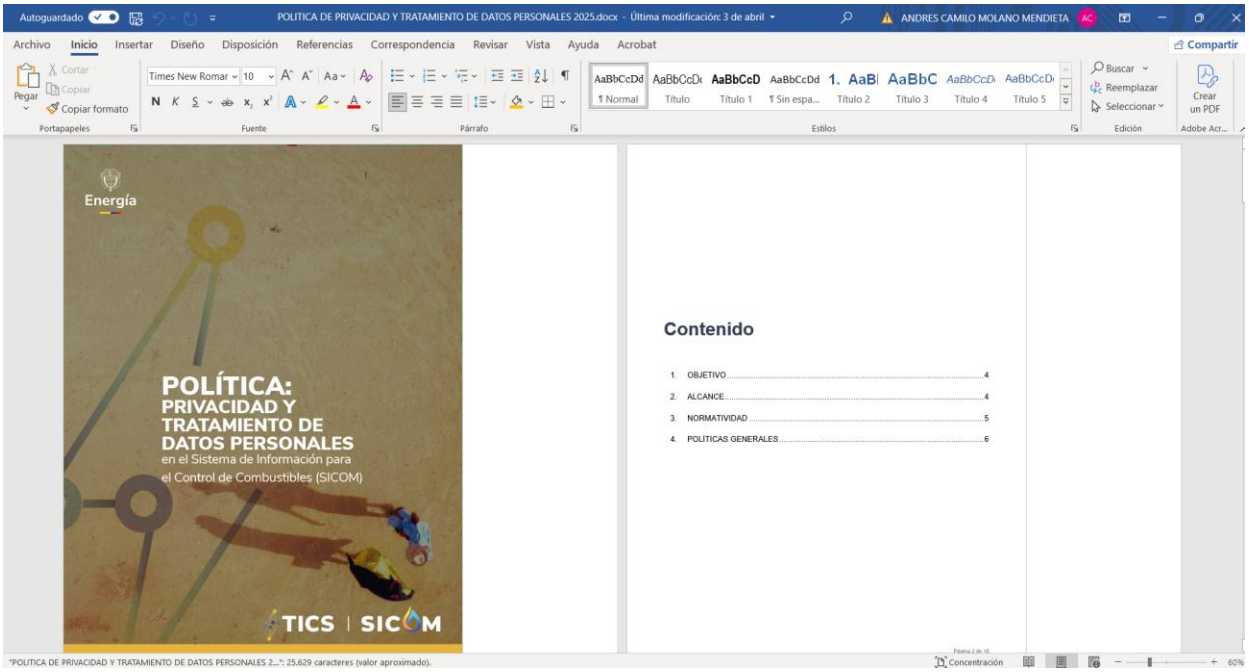


Imagen [20]. Política de privacidad y tratamiento de datos personales SICOM.

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 primer trimestre de la vigencia 2025, se avanzó en la estructuración documental de las dos primeras iniciativas estratégicas. Esto incluyó la elaboración del anexo técnico, los estudios previos y los requerimientos funcionales necesarios para llevar a cabo los procesos de contratación correspondientes, conforme a los lineamientos establecidos por la Oficina de Planeación y la normatividad vigente en contratación pública.

Es importante resaltar que estas iniciativas no solo están dirigidas a la adquisición de tecnologías específicas, sino que forman parte de un enfoque integral que contempla el fortalecimiento del recurso humano, la formalización de procesos y el desarrollo de capacidades institucionales. Todo ello con el propósito de garantizar un entorno de información seguro, resiliente y preparado para enfrentar los desafíos actuales y futuros en materia de seguridad y privacidad de la información.

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 primer 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 primer trimestre de 2025:

Energía

Tabla 5

Resultado de indicadores de seguridad de la información

Indicador	Definición	Fórmula	Meta	Meta	Resultado 1 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, Oficial de Cumplimiento y Oficial de Datos Personales, con resolución firmada.
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)	Incidente detectado, reportado y mitigado según los tiempos establecidos.
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	**100%** (4/4)	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%** (1/1)	Se implementó el doble factor de autenticación en el correo institucional. Actividades futuras están planificadas.

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.

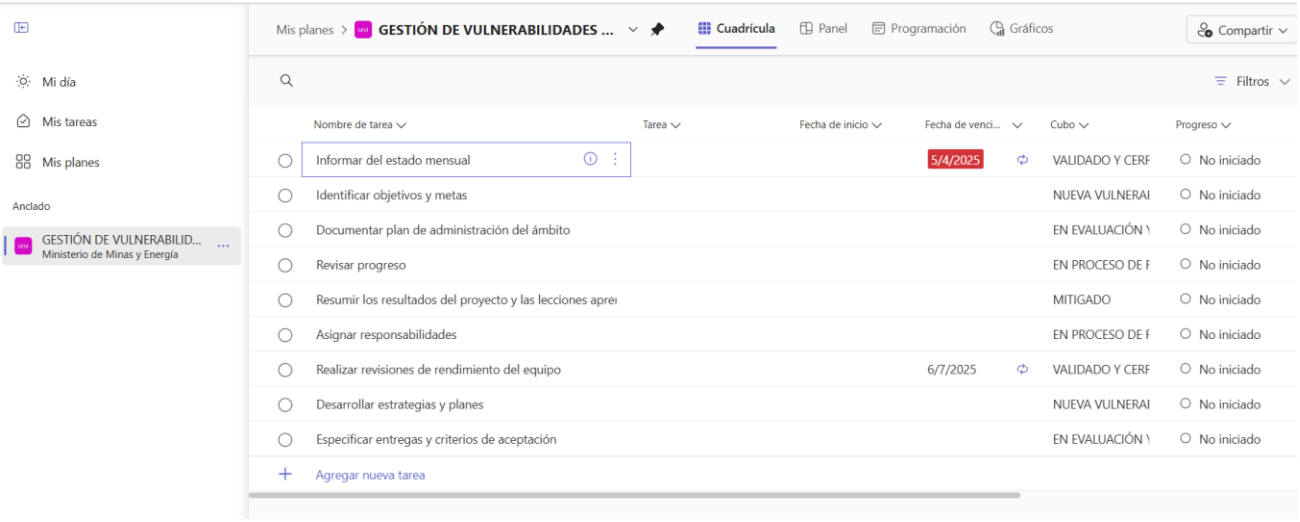
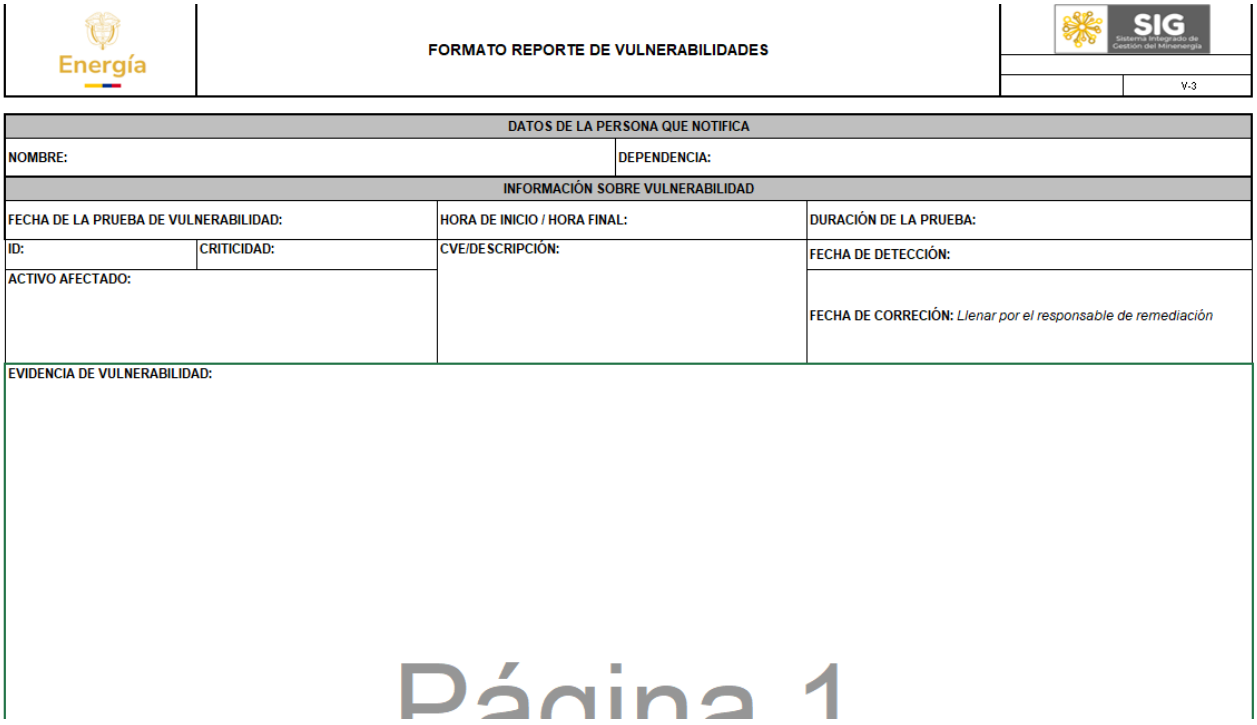


Imagen [21]. Seguimiento de gestión de vulnerabilidades con Planner.



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.

5.3 PLAN DE AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN

En cumplimiento del cronograma establecido en el Plan Anual de Auditorías Internas, se ha programado el inicio del proceso de auditoría para el Grupo de Gestión Tecnológica a partir de la primera semana de abril de 2025. Esta auditoría tiene como propósito verificar la conformidad, eficacia y oportunidad de los controles implementados en materia de seguridad de la información, así como identificar oportunidades de mejora en los procesos tecnológicos asociados.

Como resultado de esta actividad, se espera que para el segundo trimestre del año se cuente con un plan de mejora consolidado, el cual será objeto de seguimiento y verificación en todas las áreas involucradas en la gestión de la seguridad de la información. Este seguimiento permitirá fortalecer los niveles de cumplimiento normativo, madurez operativa y alineación con los lineamientos del SGSI, contribuyendo así al fortalecimiento continuo de la postura institucional frente a riesgos tecnológicos y cibernéticos.

6. CAPACITACIÓN Y SENSIBILIZACIÓN

En el marco de las actividades de fortalecimiento de la cultura organizacional en seguridad digital, y como parte de las acciones programadas en el primer trimestre de 2025, se adelantó la implementación del doble factor de autenticación (2FA) como una medida esencial para la mitigación de brechas de seguridad y el fortalecimiento de la higiene digital institucional. Esta acción, liderada por la Mesa de Ayuda en articulación con el Grupo TIC, fue dispuesta de manera obligatoria para 1.304 usuarios de la entidad. No obstante, algunos casos particulares fueron exceptuados debido a condiciones técnicas específicas o requerimientos operativos temporales, los cuales fueron debidamente justificados y documentados.

Como parte del componente de sensibilización, se programó una sesión formativa sobre la importancia del doble factor de autenticación y su rol en la protección de credenciales institucionales, la cual, aunque originalmente prevista para el primer trimestre, fue reprogramada y llevada a cabo el día 9 de abril de 2025. Durante esta sesión se abordaron aspectos clave relacionados con la cultura de higiene digital, las amenazas actuales basadas en robo de credenciales y la necesidad de adoptar medidas de protección adicionales frente a vectores de ataque cada vez más sofisticados.

A partir de esta experiencia, se encuentra actualmente en curso la planificación de temáticas para las actividades de sensibilización y formación de los próximos tres trimestres, con énfasis en las políticas internas de seguridad de la información, protocolos institucionales y temas de tendencia actual en ciberseguridad. Entre las temáticas en evaluación se destacan: manejo seguro de la información en entornos híbridos, gestión de incidentes desde el rol del usuario, riesgos asociados a

la ingeniería social, y concientización sobre el uso responsable de inteligencia artificial. Este enfoque busca consolidar una cultura de corresponsabilidad en la protección de los activos de información y fomentar prácticas seguras en todos los niveles de la organización.

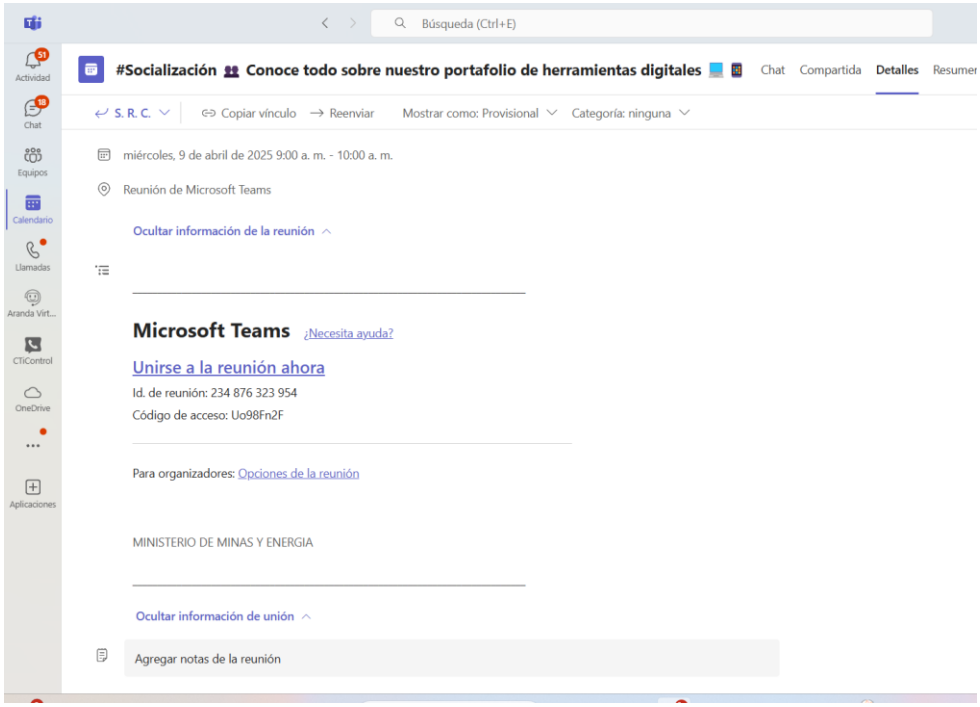


Imagen [23]. Sesión de sensibilización del doble factor de autenticación.

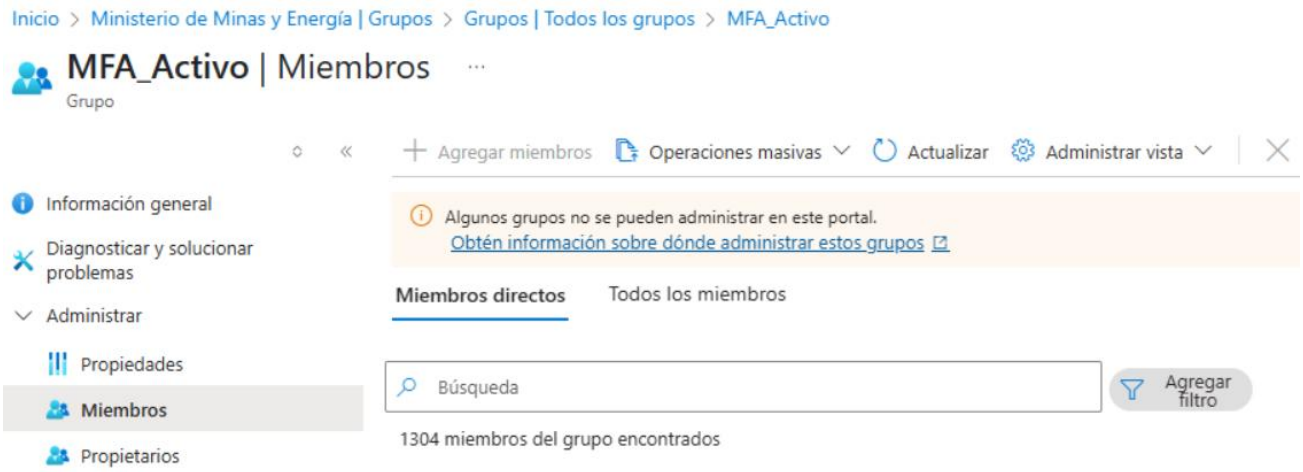


Imagen [24]. Implementación del 2FA en usuarios de la entidad.

Energía