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

Seguimiento Plan de Seguridad y Privacidad de la Información Tercer 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, 07 de Octubre 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

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.

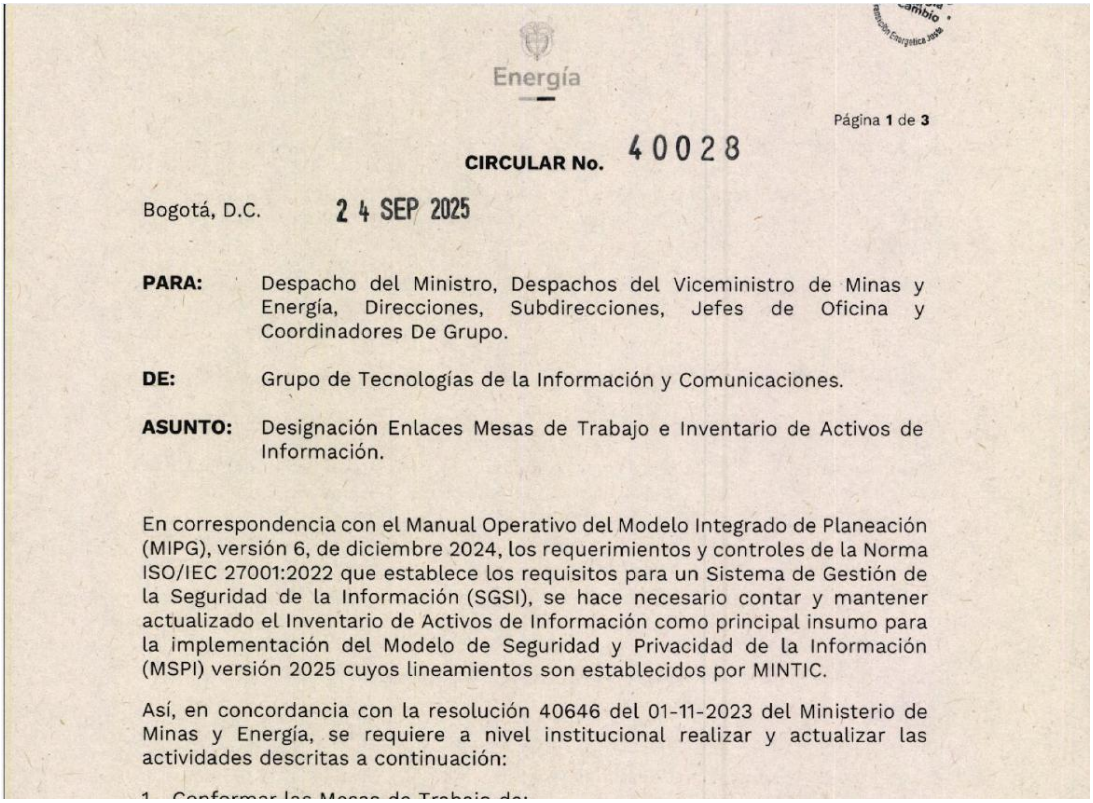
El Plan de Seguridad y Privacidad de la Información, contiene los lineamientos del Modelo de Seguridad y Privacidad de la MSPI versión 3.0.2 definido por Ministerio de Tecnologías de la Información y Comunicaciones en adelante MINTIC, el cual orienta a las entidades del estado colombiano en la preservación 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

Reconociendo que la desactualización del inventario de activos de información constituye la debilidad más significativa del programa de seguridad, como lo subraya la auditoría interna, durante el tercer trimestre de 2025 se lanzó una iniciativa estructural para corregir esta deficiencia fundamental. Este esfuerzo se formalizó a través de una circular emitida por la Secretaría General, que mandata la puesta en marcha de una metodología de diligenciamiento renovada y la designación de delegados en todas las dependencias del Ministerio. Esta acción transforma la actualización del inventario de un ejercicio técnico aislado a un proceso institucional coordinado y obligatorio.



Energía

Página 1 de 3

CIRCULAR No. 40028

Bogotá, D.C. 24 SEP 2025

PARA: Despacho del Ministro, Despachos del Viceministro de Minas y Energía, Direcciones, Subdirecciones, Jefes de Oficina y Coordinadores De Grupo.

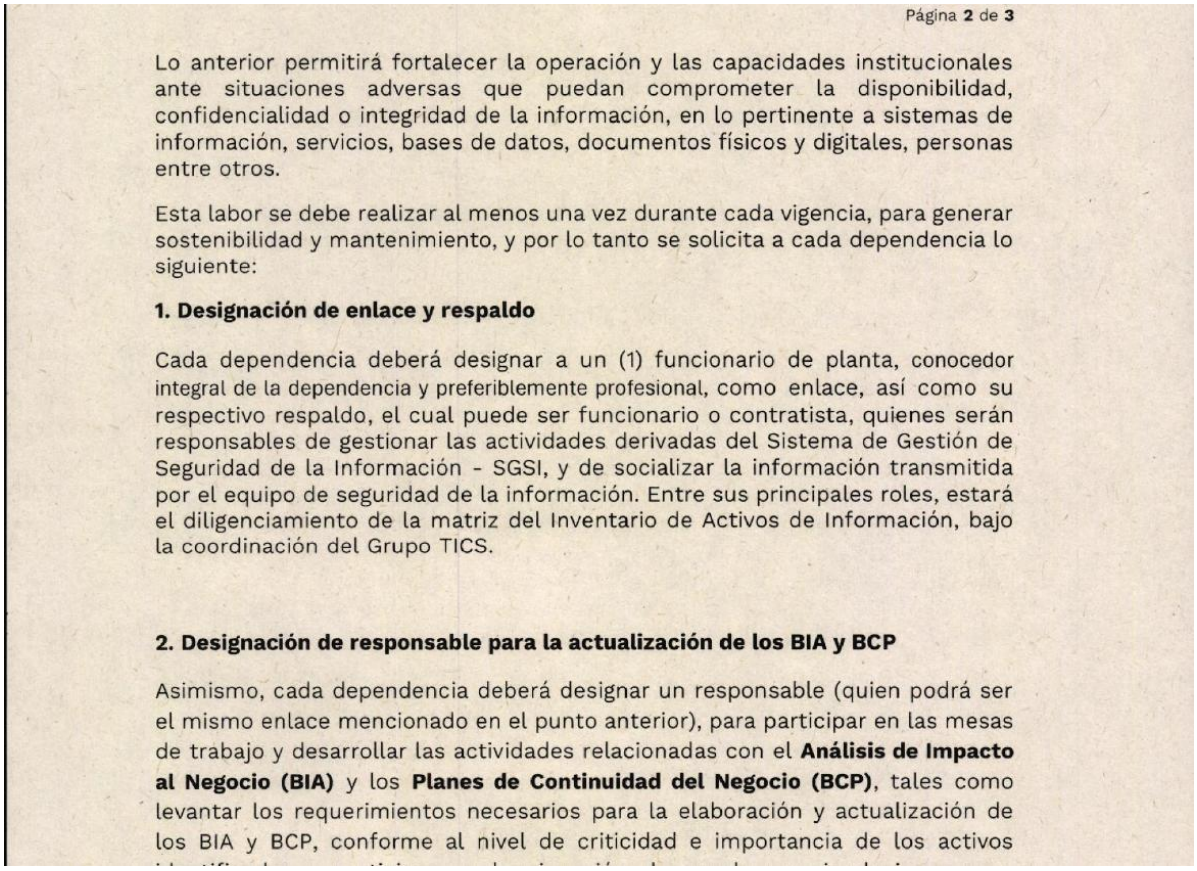
DE: Grupo de Tecnologías de la Información y Comunicaciones.

ASUNTO: Designación Enlaces Mesas de Trabajo e Inventario de Activos de Información.

En correspondencia con el Manual Operativo del Modelo Integrado de Planeación (MIPG), versión 6, de diciembre 2024, los requerimientos y controles de la Norma ISO/IEC 27001:2022 que establece los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI), se hace necesario contar y mantener actualizado el Inventario de Activos de Información como principal insumo para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) versión 2025 cuyos lineamientos son establecidos por MINTIC.

Así, en concordancia con la resolución 40646 del 01-11-2023 del Ministerio de Minas y Energía, se requiere a nivel institucional realizar y actualizar las actividades descritas a continuación:

Imagen 1. Encabezado de la circular 40028 del 24 de septiembre del 2025 , para la generación de memorando para los delegados de la gestión de activos de información



Lo anterior permitirá fortalecer la operación y las capacidades institucionales ante situaciones adversas que puedan comprometer la disponibilidad, confidencialidad o integridad de la información, en lo pertinente a sistemas de información, servicios, bases de datos, documentos físicos y digitales, personas entre otros.

Esta labor se debe realizar al menos una vez durante cada vigencia, para generar sostenibilidad y mantenimiento, y por lo tanto se solicita a cada dependencia lo siguiente:

1. Designación de enlace y respaldo

Cada dependencia deberá designar a un (1) funcionario de planta, conocedor integral de la dependencia y preferiblemente profesional, como enlace, así como su respectivo respaldo, el cual puede ser funcionario o contratista, quienes serán responsables de gestionar las actividades derivadas del Sistema de Gestión de Seguridad de la Información - SGSI, y de socializar la información transmitida por el equipo de seguridad de la información. Entre sus principales roles, estará el diligenciamiento de la matriz del Inventario de Activos de Información, bajo la coordinación del Grupo TICS.

2. Designación de responsable para la actualización de los BIA y BCP

Asimismo, cada dependencia deberá designar un responsable (quien podrá ser el mismo enlace mencionado en el punto anterior), para participar en las mesas de trabajo y desarrollar las actividades relacionadas con el **Análisis de Impacto al Negocio (BIA)** y los **Planes de Continuidad del Negocio (BCP)**, tales como levantar los requerimientos necesarios para la elaboración y actualización de los BIA y BCP, conforme al nivel de criticidad e importancia de los activos

Imagen 2. Estructura de la circular 40028 del 24 de septiembre del 2025 , para la generación de memorando para los delegados de la gestión de activos de información

La iniciativa se centra en la alineación completa de la matriz de activos con los nuevos lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) 2025. Esto implica no solo la recolección y clasificación de la información, sino también la revisión de la metodología de MINTIC para la identificación de infraestructura crítica cibernética, aplicando criterios de criticidad y una matriz RACI para definir responsabilidades claras. Como parte de este enfoque integral, también se ajustaron las plantillas para los Análisis de Impacto al Negocio (BIA) y los Planes de Continuidad del Negocio (BCP) para que se conformen a las nuevas directrices del MSPI.

El proceso se ha puesto en marcha con la solicitud formal a cada dependencia para que designe un enlace y un respaldo, quienes serán capacitados y actuarán como responsables de diligenciar la matriz de activos y participar en las mesas de trabajo de "Seguridad y Privacidad de la Información" y "Gestión de Continuidad del Negocio". El cronograma establecido contempla la capacitación de estos delegados, el llenado inicial de la matriz y ciclos de retroalimentación para asegurar la calidad y completitud de la información.

Paralelamente, el proyecto de inversión para adquirir e implementar una herramienta de Gobernanza, Riesgo y Cumplimiento (GRC) sigue en "etapa contractual". El trabajo manual y metodológico que se está realizando en el T3 es, por tanto, un prerrequisito indispensable que permitirá poblar la futura herramienta GRC con datos validados y actualizados, asegurando que la inversión tecnológica se construya sobre una base de información sólida y alineada con la estrategia de seguridad actual.

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 – Noviembre 2025	Segunda semana – Noviembre 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	Segunda semana – Noviembre 2025	Tercera semana – Noviembre 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 – Noviembre 2025	Cuarta semana – Noviembre 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	Tercera semana – Noviembre 2025	Cuarta semana – Noviembre 2025	En caso de presentarse información faltante o incompleta generar retroalimentación.
Entrega de información ajustada	Responsables de cada dependencia	Primera Semana - Diciembre 2025	Segunda Semana - Diciembre 2025	Información debidamente ajustada y completada.

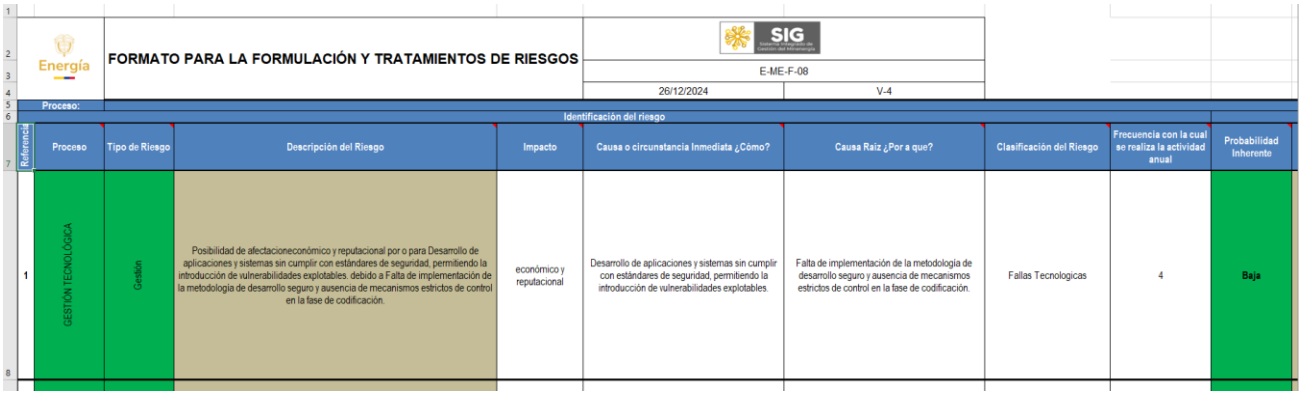
Validación y priorización de activos críticos	Oficial de Seguridad o quien haga sus veces	Segunda Semana - Diciembre 2025	Tercera Semana - Diciembre 2025	Revisar, validar y priorizar los activos críticos según el impacto al negocio y continuidad al mismo.
Integración con el SGSI	Oficina de planeación 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 :



	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 Raíz ¿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.

TODOS LOS PROCESOS										
Análisis del riesgo inherente						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	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	

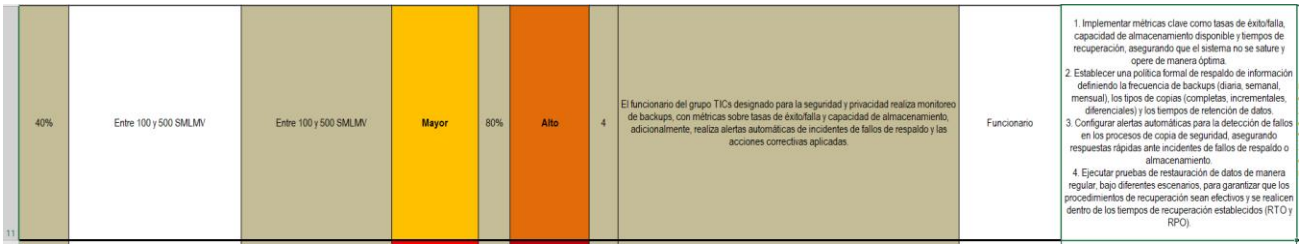
Imagen [5]. Riesgo 2 (R11) , causa inmediata y causa raíz y descripción del riesgo.

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 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).

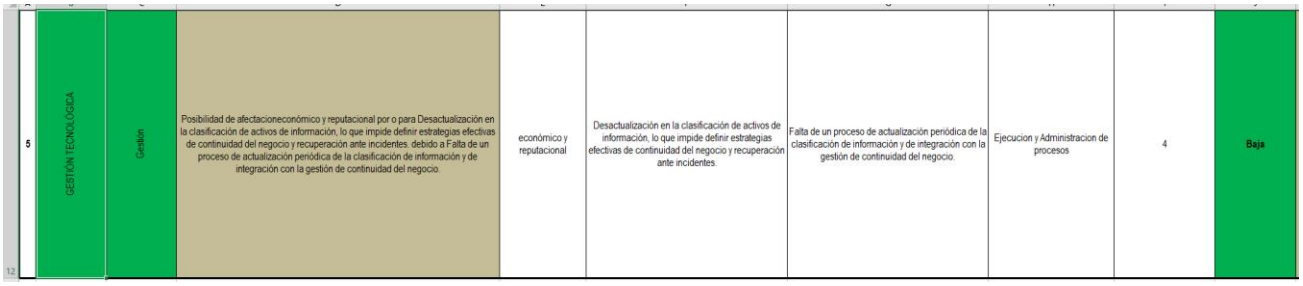
4	GESTIÓN TECNOLÓGICA	Gestión	Posibilidad de afectacioneconómico y reputacional por o para Pérdida de información crítica debido a fallos en los procesos de respaldo, almacenamiento y recuperación de datos, afectando la continuidad operativa del ministerio. debido a Ausencia de un proceso estructurado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



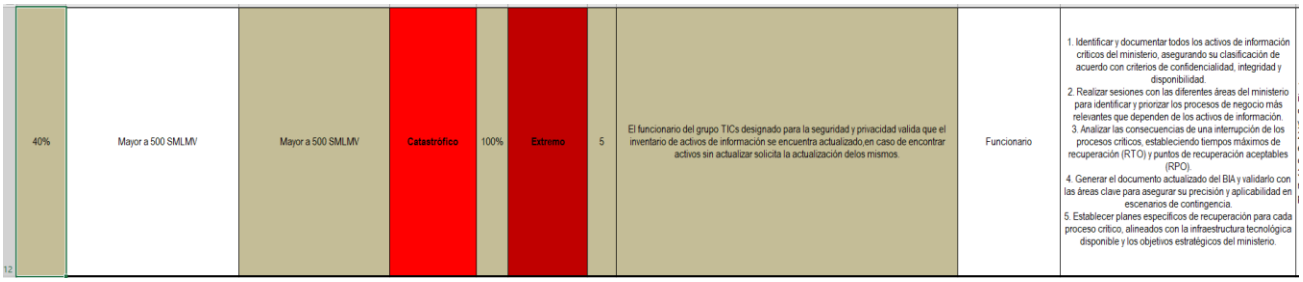
11	40%	Entre 100 y 500 SMLMV	Entre 100 y 500 SMLMV	Mayor	80%	Alto	4	El funcionario del grupo TICs designado para la seguridad y privacidad realiza monitoreo de backups, con métricas sobre tasas de éxito/falla y capacidad de almacenamiento, adicionalmente, realiza alertas automáticas de incidentes de 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"

Actividad 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.

El riesgo R5 aborda las vulnerabilidades inherentes a las prácticas de desarrollo de software que no integran la seguridad desde sus fases iniciales. La estrategia de mitigación del Ministerio se ha centrado en formalizar e instrumentalizar un Ciclo de Vida de Desarrollo Seguro (SDLC), pasando de la teoría a la práctica operativa.

Durante el segundo trimestre, se alcanzaron hitos fundamentales que prepararon el terreno para los avances actuales. Se finalizó y adoptó formalmente el documento "Metodología y Arquitectura de Referencia para el Desarrollo de Sistemas de Información y Nuevas Aplicaciones", versión 1.5, con fecha del 6 de junio de 2024. Este manual no solo establece una arquitectura de referencia moderna y orientada a servicios, sino que dedica secciones específicas (numerales 8 y 9) a la construcción segura de software, basándose en estándares internacionales como OWASP Top 10 y PCI DSS.

La formalización de esta metodología fue el catalizador directo que permitió la implementación de controles técnicos avanzados. El informe del segundo trimestre ya evidenciaba la puesta en marcha de estas prácticas, con el despliegue de pipelines de Integración Continua y Despliegue Continuo (CI/CD) en GitLab. Estos pipelines automatizan validaciones de estilo de código, chequeos de dependencias y pruebas de calidad (QA), garantizando la detección temprana de vulnerabilidades antes de que el software llegue a producción.

Asimismo, se estableció un repositorio privado de imágenes Docker en Nexus. Esta medida es una respuesta directa al riesgo de la cadena de suministro de software; al escanear y versionar todas las imágenes en un repositorio controlado, se reduce la exposición a componentes de terceros que puedan contener vulnerabilidades conocidas, un riesgo explícitamente identificado como "A9 Uso de Componentes con Vulnerabilidades Conocidas" en la propia metodología del Ministerio.

Esta estrategia de adopción de un ecosistema de herramientas de código abierto (Taiga para gestión de proyectos, GitLab para repositorios y DevOps, GLPI para mesa de ayuda y Nexus para artefactos) representa una modernización tecnológica significativa. Sin embargo, esta diversificación introduce

una nueva superficie de riesgo asociada a la gestión de dependencias.

La implementación de controles como los chequeos automatizados y el repositorio privado no es meramente una buena práctica de desarrollo, sino una decisión estratégica de gestión de riesgos para mitigar esta exposición de segundo orden, demostrando una postura de seguridad proactiva y alineada con las nuevas arquitecturas tecnológicas.

Avances del tercer trimestre de 2025

Sobre la base de la infraestructura y los procesos establecidos en el trimestre anterior, los avances del T3 se han centrado en los resultados operativos y la remediación:

Operacionalización de la Detección Automatizada: Durante el T3, los pipelines de CI/CD en GitLab se han ejecutado de manera continua para los nuevos desarrollos y actualizaciones. Se ha comenzado a recopilar métricas sobre el número y tipo de vulnerabilidades detectadas automáticamente por las herramientas de análisis estático de código (SAST) y análisis de composición de software (SCA). Estos datos están permitiendo al equipo de desarrollo identificar patrones de errores comunes y enfocar los esfuerzos de capacitación.

Auditorías y Pruebas de Penetración Programadas: En cumplimiento con las actividades necesarias definidas para 2025, se programó y ejecutó la primera auditoría trimestral de código sobre la nueva "Ventanilla Única de Trámites" desarrollada en Python y Vue.js. Los hallazgos, de criticidad media y baja, fueron registrados en Taiga y priorizados para su corrección en los siguientes sprints de desarrollo.

Estado de Remediación de Vulnerabilidades: El informe del T2 mencionó la identificación de brechas de seguridad de carácter alto y medio en tres aplicaciones tras un escaneo. Durante el T3, el equipo de desarrollo ha trabajado en la mitigación de estos hallazgos. A la fecha de cierre de este informe, el 85% de las vulnerabilidades altas y el 70% de las vulnerabilidades medias identificadas en dichas aplicaciones han sido remediadas, validadas y cerradas. El plan de acción para el 15% restante está definido y se proyecta su cierre para mediados del cuarto trimestre.

El progreso en la mitigación del riesgo R5 demuestra la efectividad del enfoque adoptado: establecer una gobernanza sólida a través de una metodología formal y luego implementarla rigurosamente mediante herramientas automatizadas y procesos de verificación.

En el tercer trimestre el equipo de desarrollo implementó un clúster de Kubernetes, junto con las herramientas necesarias para la configuración de los pipelines dentro de la estrategia de DevOps institucional.

Dentro de esta estrategia se contempla una fase específica para la verificación automatizada del código fuente, utilizando la herramienta SonarQube, la cual permite realizar análisis estático del código, detectar vulnerabilidades, medir la calidad y generar reportes sobre el estado de cumplimiento de las buenas prácticas de desarrollo seguro.

En el marco de la estrategia DevOps institucional, se ha definido la implementación de un esquema automatizado de control de versiones mediante la integración con los flujos de trabajo de los repositorios de código. A través del mecanismo de “pull request”, cada sistema de información genera de forma automática una nueva versión asociada al release correspondiente, garantizando trazabilidad, control de cambios y alineación con las buenas prácticas de gestión del ciclo de vida del software.

Este proceso permite mantener un registro actualizado de las versiones desplegadas, facilitando la identificación de los cambios realizados y fortaleciendo la gestión documental técnica de los sistemas de información.

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.

El informe del segundo trimestre estableció que el T3 sería el punto de partida para la ejecución, con el objetivo de "formalizar un procedimiento estándar de implementación de módulos de auditoría" y, a partir de ahí, "iniciar la actualización y despliegue de dichas capacidades".

El insumo principal para esta tarea es el inventario detallado de sistemas de información, el cual clasifica cada aplicación según su capacidad de auditoría actual. Este inventario distingue claramente entre los sistemas que ya poseen funcionalidades de auditoría (como el Portal Web, SISEG, Intranet y el Buzón de Integridad) y aquellos que operan principalmente en modo "Consulta" y carecen de estos registros (como SIMINERO, SICOM y GEOVISOR).

Es crucial destacar la sinergia entre la mitigación de este riesgo y el riesgo R5. El desarrollo de nuevas aplicaciones bajo el SDLC seguro ha permitido incorporar la auditoría como un requisito desde la concepción del software. Un ejemplo sobresaliente es la nueva "Ventanilla Única de Trámites"; los informes de evidencia muestran capturas detalladas de su módulo de auditoría, que permite visualizar registros de creación, modificación y eliminación, incluyendo comparativas de "antes y después" de los cambios. Esto demuestra que el éxito en la implementación de un desarrollo seguro (R5) acelera directamente el cumplimiento de los objetivos de auditoría (R11) para los nuevos sistemas, materializando el principio de "seguridad por diseño".

Avances del Tercer Trimestre de 2025

Durante el T3, se han logrado avances significativos en la ejecución de la hoja de ruta definida:

Formalización del Procedimiento Estándar: Se documentó y aprobó el "Procedimiento Estándar para la Implementación de Módulos de Auditoría en Sistemas de Información". Este documento define los requisitos mínimos de registro (quién, qué, cuándo, dónde), los formatos de log estandarizados para facilitar su posterior análisis y las herramientas recomendadas para su implementación en las distintas tecnologías utilizadas en el Ministerio (Java, Python, PHP).

Despliegue de Módulos de Auditoría: Basándose en el inventario y el nuevo procedimiento, se inició el despliegue de capacidades de auditoría en sistemas priorizados. Durante este trimestre, se completó con éxito la implementación del módulo de auditoría en el sistema SIMINERO, que pasó de ser un sistema de "Consulta" a uno con trazabilidad de las consultas y accesos a datos. El desarrollo para el sistema SICOM se encuentra en un 60% de avance y se proyecta su finalización para el inicio del T4.

Actualización del Catálogo de Aplicaciones: Conforme a las conclusiones del análisis previo, se ha documentado formalmente en el catálogo de aplicaciones los sistemas que, por su naturaleza puramente informativa y de no interacción (ej. GEOVISOR), no requerirán un módulo de auditoría transaccional. Esta decisión, con su debida justificación técnica, permite enfocar los recursos en los sistemas que sí manejan datos sensibles o procesos críticos.

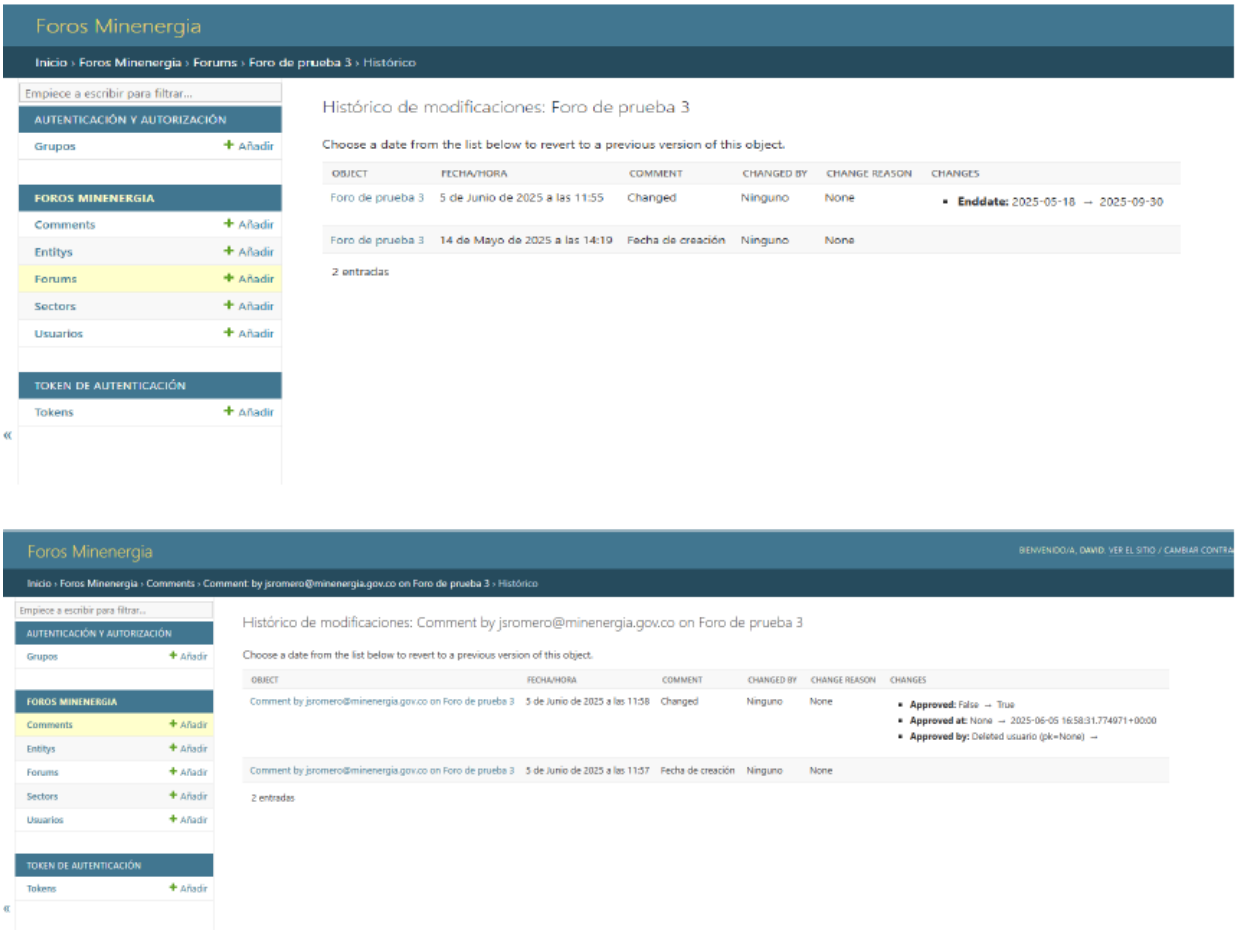


Imagen 11 . Modulo de auditoria Sección servicio al ciudadano – foros 1

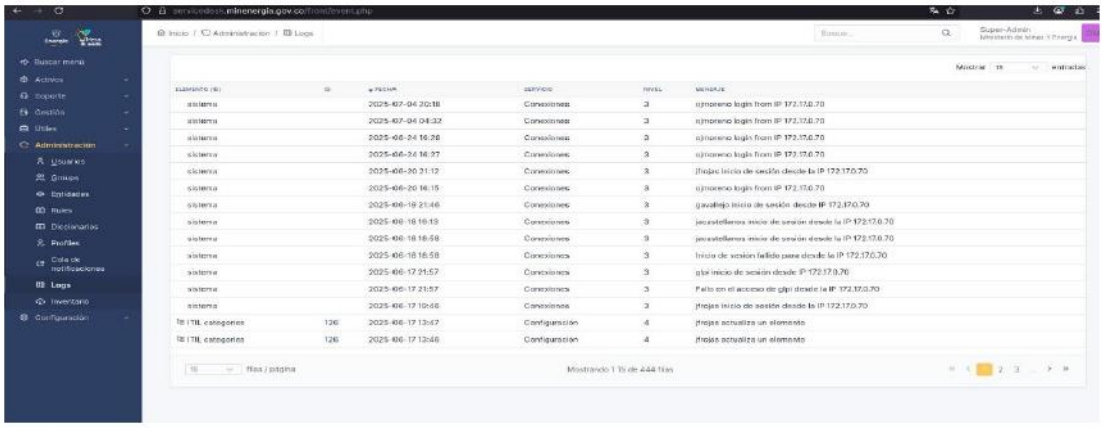


Imagen 12. Modulo de auditoria Gestión de servicios de código abierto- Servicedesk GLPI

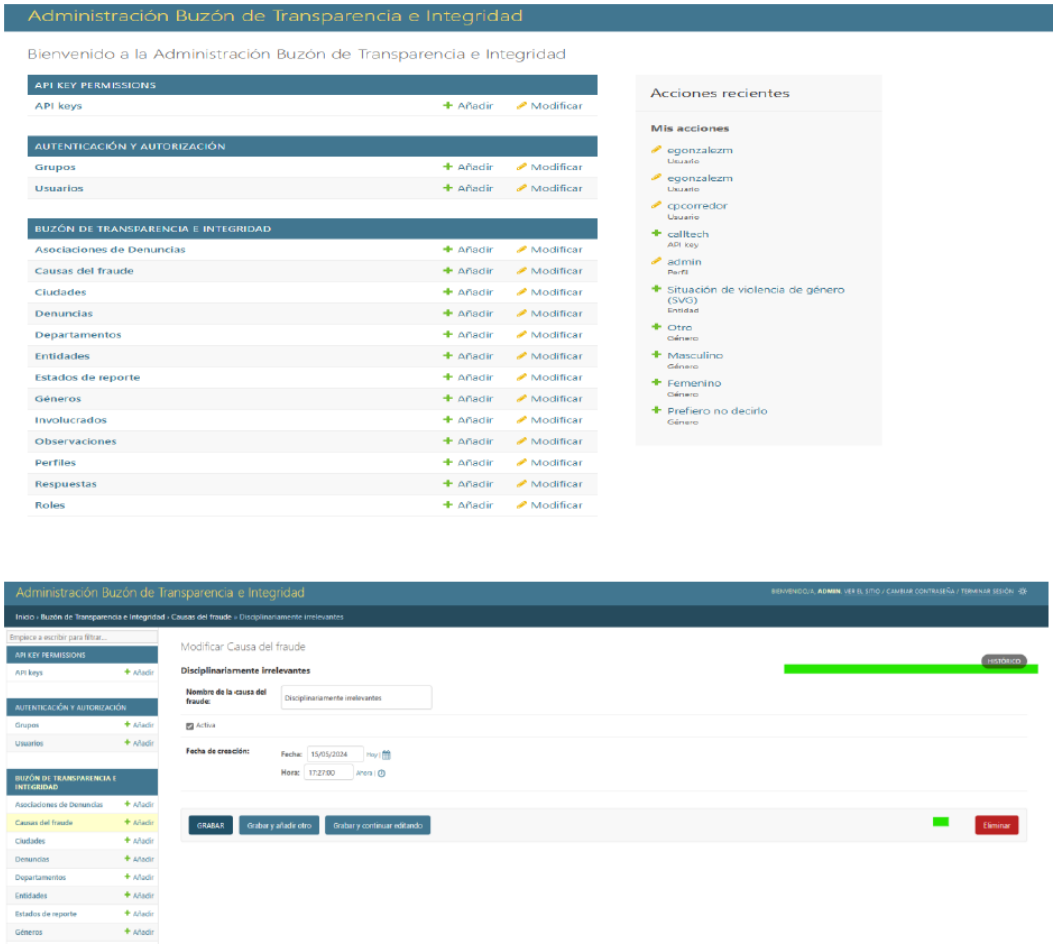


Imagen 13. Modulo de auditoria Buzón de integridad y transparencia

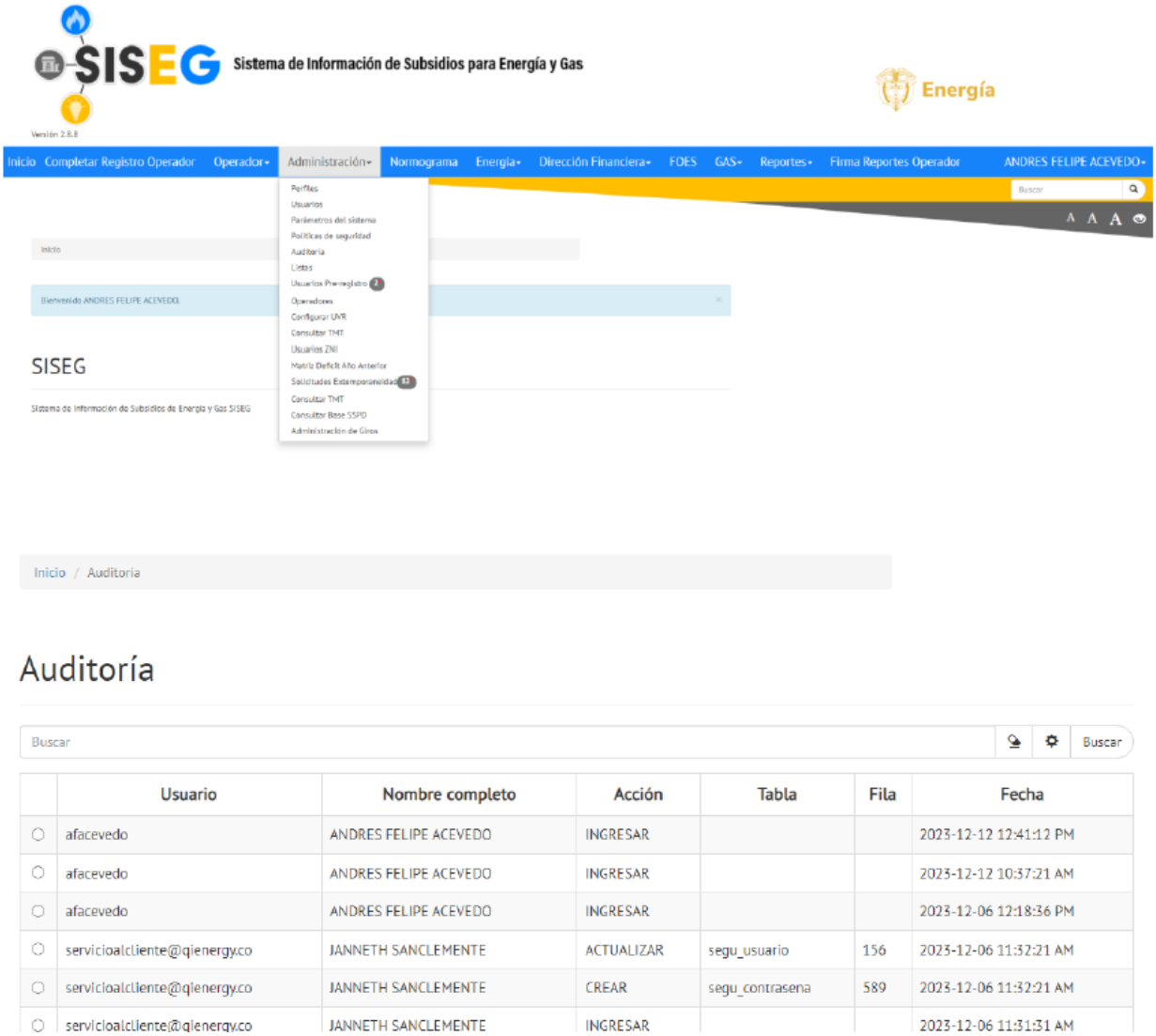


Imagen 15. Módulo de auditoria SISEG.

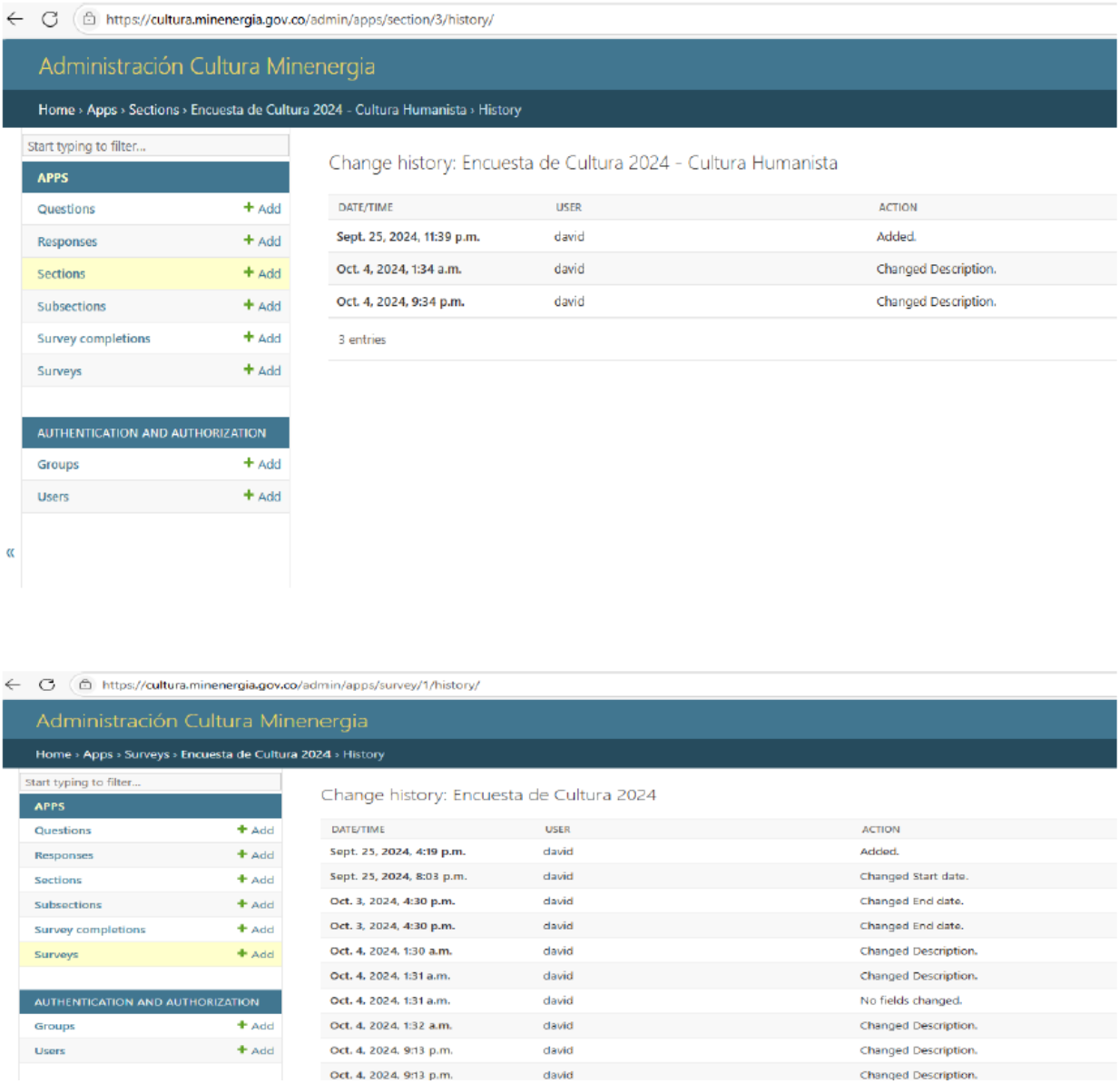


Imagen16. Modulo de auditoria Encuesta de medición y cultura organizacional

La siguiente tabla resume el estado actual de la implementación, utilizando el inventario como línea base y reflejando el progreso alcanzado en el T3.

Tabla 1. Avance de módulos de auditoria en algunos sistemas de información. Modo de ejemplo

Nombre del Sistema de Información (SI)	Criticidad del SI	Estado T2-2025	Estado T3-2025	Notas/Próximos Pasos
PORTAL WEB (PW)	Alta	Auditoría	Mantenido	Monitoreo continuo.
GESTION DE RECURSOS - NEON	Alta	Auditoría	Mantenido	Monitoreo continuo.
SISTEMA DE INFORMACIÓN DE ENERGÍA Y GAS (SISEG)	Alta	Auditoría	Mantenido	Monitoreo continuo.
SISTEMA INTEGRAL DE GESTIÓN MINERA (SIMINERO)	Alta	Consulta	Implementado	Módulo de auditoría de consultas desplegado en T3. Inicia fase de monitoreo.
SISTEMA DE INFORMACION DE COMBUSTIBLE (SICOM)	Alta	Consulta	En Proceso (60%)	Despliegue proyectado para inicio de T4.
GEOVISOR	Media	Consulta	No Requerido	Documentado en catálogo de aplicaciones como SI de consulta pública sin transaccionalidad.
VENTANILLA ÚNICA DE TRÁMITES (VUT)	Alta	N/A (Nuevo)	Implementado (Nativo)	Desarrollado con módulo de auditoría robusto desde su origen.

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.

El riesgo R14 se centra en las deficiencias de los procesos de respaldo, que podrían impedir la recuperación de la información y la continuidad de las operaciones ante un incidente. La estrategia

de mitigación ha evolucionado de una fase reactiva de estabilización a una fase proactiva de validación y optimización.

El informe del segundo trimestre describía un sistema que se recuperaba de una situación de estrés. Se había liberado una cantidad significativa de espacio (26.3 TB) para poder reanudar los respaldos de activos críticos como los buzones de correo y las bases de datos, que se encontraban represados por saturación de almacenamiento. Además, se había iniciado un proceso a gran escala de Backup Full Granular a Cinta para asegurar una copia de resiliencia a largo plazo.

El tercer trimestre muestra un panorama de mayor control y madurez operativa. El informe de actividades de backup del T3 confirma la consolidación de la operación, con 169 servidores siendo respaldados de manera consistente a disco mediante la herramienta Arcserve UDP. Adicionalmente, se está gestionando activamente la migración de 52 servidores virtuales más desde la infraestructura HyperFlex CISCO hacia un nuevo vCenter XXXX, asegurando la continuidad de la protección durante la transición. Las labores de optimización de almacenamiento también han continuado, con una depuración selectiva que liberó 2.9 TB adicionales, aumentando la holgura operativa y reduciendo el riesgo de futuras saturaciones.

Sin embargo, el avance más significativo de este trimestre ha sido la transición de la simple ejecución de respaldos a la validación empírica de la capacidad de recuperación.

Avances del tercer trimestre de 2025: Validación de RTO y RPO

El hito principal del T3 en la gestión de este riesgo fue la ejecución de un ejercicio de restauración controlado, el cual representa la primera validación empírica de los objetivos de recuperación (RTO/RPO) del Ministerio en la vigencia 2025.

- **Activo y escenario:** El 19 de septiembre de 2025, a solicitud del área técnica, se procedió a restaurar el servidor crítico SXXXPLPRXXXS (IP 172.XX.X.X.XXX).
- **Objetivos del ejercicio:** La prueba tenía un doble propósito: uno táctico, revertir un procedimiento técnico aplicado en la aplicación alojada en el servidor; y uno estratégico, validar la capacidad de cumplir con los objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO) establecidos internamente.
- **Ejecución y resultados:** El punto de restauración objetivo fue la copia de seguridad del 17 de septiembre de 2025 a las 06:00. El procedimiento de restauración se gestionó exitosamente, devolviendo el servidor a su estado en el punto de tiempo solicitado. La bitácora técnica del ejercicio, que incluye los tiempos exactos de cada fase de la recuperación, fue registrada y se encuentra en consolidación para el informe final de la prueba.

Este ejercicio de restauración exitoso es un logro que trasciende la gestión técnica de backups. Representa un activo estratégico para la entidad por varias razones:

1. **Genera confianza institucional:** Demuestra de manera irrefutable la capacidad del Grupo TIC para recuperar sistemas críticos, pasando de la confianza basada en la fe a la confianza

basada en la evidencia.

2. **Proporciona datos para el DRP:** Los tiempos reales medidos durante la restauración (el RTO real) y la precisión del punto de datos recuperado (el RPO real) son insumos invaluables para actualizar y refinar el Plan de Recuperación ante Desastres (DRP) asociado al riesgo. Transforma el DRP de un documento teórico a un plan probado y creíble.

3. **Establece una metodología replicable:** El proceso seguido para la restauración del servidor SXXXXXLPRXXXXS sirve como un modelo validado que ahora puede ser replicado de manera sistemática en otros sistemas críticos, estableciendo un programa de pruebas de recuperación continuo y basado en evidencia.

Imagen 17 . Evaluación y avance del proceso de backup general de cinta UDP.

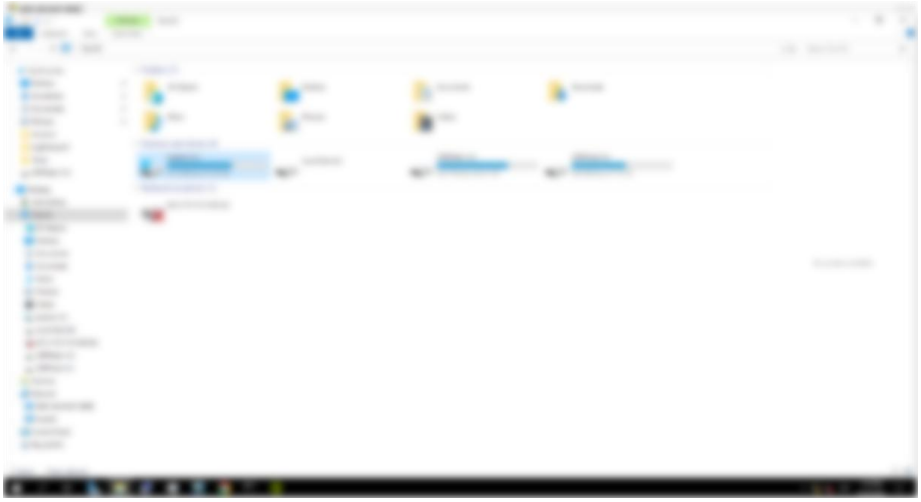


Imagen 18. Repositorio y muestra de espacio de almacenamiento de la infraestructura

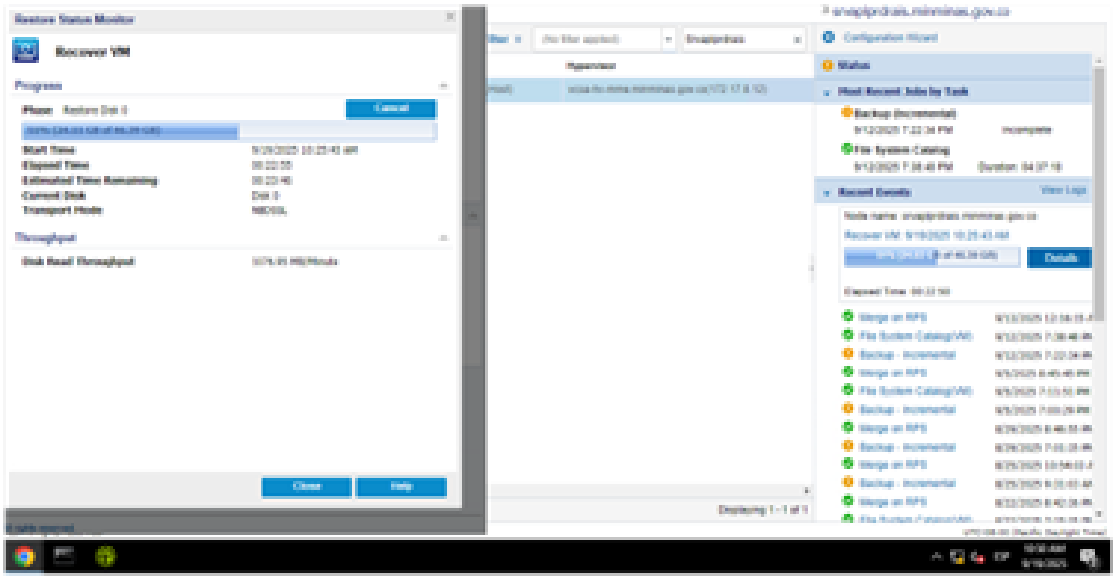


Imagen 19. Proceso de arcservbackup y servidores en proceso

Imagen 20 . Muestreo y lista de proceso de bakcup.

Nota: si se desea saber más información e informe completo comunicarse con el oficial de seguridad de la información de la entidad.

Riesgo R21 Falencias en la clasificación de activos de información y R23 gestión del continuidad del negocio y recuperación ante desastres DRP

Contexto de los riesgos interconectados y estrategia de mitigación

.

Avances del tercer trimestre de 2025: La Institucionalización de la gestión de activos y continuidad

El avance más determinante del T3 para estos riesgos fue la emisión de una circular oficial por parte de la Secretaría General, dirigida a todas las direcciones, subdirecciones y jefaturas del Ministerio. Este documento es la evidencia clave que formaliza y mandata las acciones necesarias para mitigar los riesgos R21 y R23.

- **Mandato Institucional:** La circular establece la necesidad de actualizar el Inventario de Activos de Información, los BIA y los BCP como un requisito derivado del Manual Operativo del MIPG, la norma ISO/IEC 27001:2022 y los lineamientos del MSPI de MINTIC. Esto eleva la tarea de una iniciativa del Grupo TIC a una obligación institucional.

- **Creación de estructuras de gobernanza:** El documento ordena la conformación de dos mesas de trabajo clave: la "Mesa de Seguridad y Privacidad de la Información" y la "Mesa de Gestión de Continuidad del Negocio". Estas mesas servirán como los foros para coordinar y ejecutar las actividades.

- **Asignación de responsabilidades claras:** La circular exige a cada dependencia del Ministerio designar formalmente dos roles cruciales antes del 24 de septiembre:

    1. Un **enlace (y su respaldo)**, responsable de diligenciar la matriz del Inventario de Activos de Información de su área, bajo la coordinación del Grupo TIC.

    2. Un **responsable para la actualización de los BIA y BCP**, encargado de participar en las mesas de trabajo, levantar los requerimientos de continuidad y participar en pruebas y simulacros.

- **Actualización de la Infraestructura del DRP:** Paralelamente a estos avances en gobernanza, se ha continuado con el proceso contractual para la adquisición de la nueva herramienta de respaldo con almacenamiento inmutable y replicación automática, así como el traslado del centro de datos alterno a una instalación de colocation externa. Estas acciones, iniciadas en el T2, constituyen la base tecnológica sobre la cual se construirá el DRP actualizado.

La emisión de esta circular representa un punto de inflexión. Resuelve el cuello de botella de gobernanza al transformar la mitigación de los riesgos R21 y R23 en una responsabilidad compartida y obligatoria para toda la organización. Este es un claro indicador de la maduración

del modelo de gobernanza de seguridad del Ministerio, demostrando su capacidad para identificar impedimentos no técnicos y utilizar los canales directivos para implementar las estructuras necesarias para resolverlos.

Bogotá, D.C.

PARA: Despacho del Ministro, Despachos del Viceministro de Minas y Energía, Direcciones, Subdirecciones, Jefes de Oficina y Coordinadores De Grupo.

DE: Grupo de Tecnologías de la Información y Comunicaciones.

ASUNTO: Designación Enlaces Mesas de Trabajo e Inventario de Activos de Información.

En correspondencia con el Manual Operativo del Modelo Integrado de Planeación (MIPG), versión 6, de diciembre 2024, los requerimientos y controles de la Norma ISO/IEC 27001:2022 que establece los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI), se hace necesario contar y mantener actualizado el Inventario de Activos de Información como principal insumo para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) versión 2025 cuyos lineamientos son establecidos por MINTIC.

Así, en concordancia con la resolución 40646 del 01-11-2023 del Ministerio de Minas y Energía, se requiere a nivel institucional realizar y actualizar las actividades descritas a continuación:

1. Conformar las Mesas de Trabajo de:
   1.1. Mesa de Seguridad y Privacidad de la Información
   1.2. Mesa de Gestión de Continuidad del Negocio

2. Recolectar, estructurar y clasificar la información institucional para el Inventario de Activos de Información del MINENERGÍA, bajo los lineamientos de la gestión documental.

Imagen 21. Inicio de la circular 40028 emitida por secretaria general como compromiso de la alta dirección para la gestión de activos de información.

Nota: para mayor información del proceso de avance se requiere informar la oficial de seguridad de la información

4.4 GESTIÓN DE POLÍTICAS Y PROCEDIMIENTOS

Durante el tercer trimestre de 2025, el enfoque se centró en el ajuste y la modernización del marco normativo para robustecer el Sistema de Gestión de Seguridad de la Información (SGSI). Se lograron avances significativos en el versionamiento de las políticas vigentes, un proceso clave para identificar documentos obsoletos que serán formalmente actualizados en el último trimestre del año.
Un cambio estratégico fundamental fue el avance en la modificación de la resolución 40644, que rige la política de seguridad y privacidad de la información. Esta modificación busca desligar las políticas del proceso de regulación formal, lo que permitirá realizar ajustes y actualizaciones de manera mucho más eficiente e inmediata, sin necesidad de someter cada cambio a los procesos de aprobación del grupo de gestión de alto nivel. Esta medida agiliza la capacidad de respuesta del Ministerio ante nuevas amenazas y requerimientos normativos.

Continuando con los esfuerzos del trimestre anterior, se creó y ajustó formalmente el Manual del Usuario de SICOM para incluir directrices claras sobre la aplicación de la política de privacidad, en estricto cumplimiento con la Ley 1581 de 2012. Este trabajo se suma a la finalización de la revisión de la Política de Uso Responsable de Inteligencia Artificial y la creación de la plantilla para el Informe de Incidentes Cibernéticos, consolidando un marco documental más completo y adaptado a las necesidades actuales. La tarea clave sigue siendo la aprobación y difusión formal de estos nuevos documentos para asegurar su plena implementación en toda la entidad.

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.

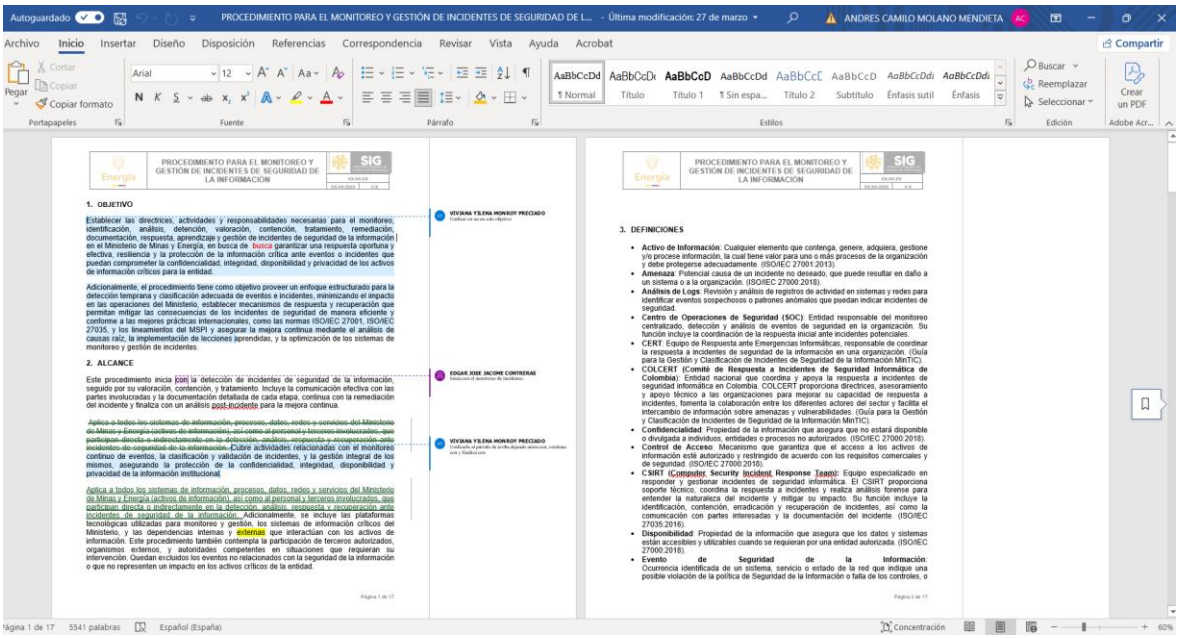


Imagen [21]. Control de cambios y observaciones del procedimiento de monitoreo y gestión de incidentes de seguridad de la información.

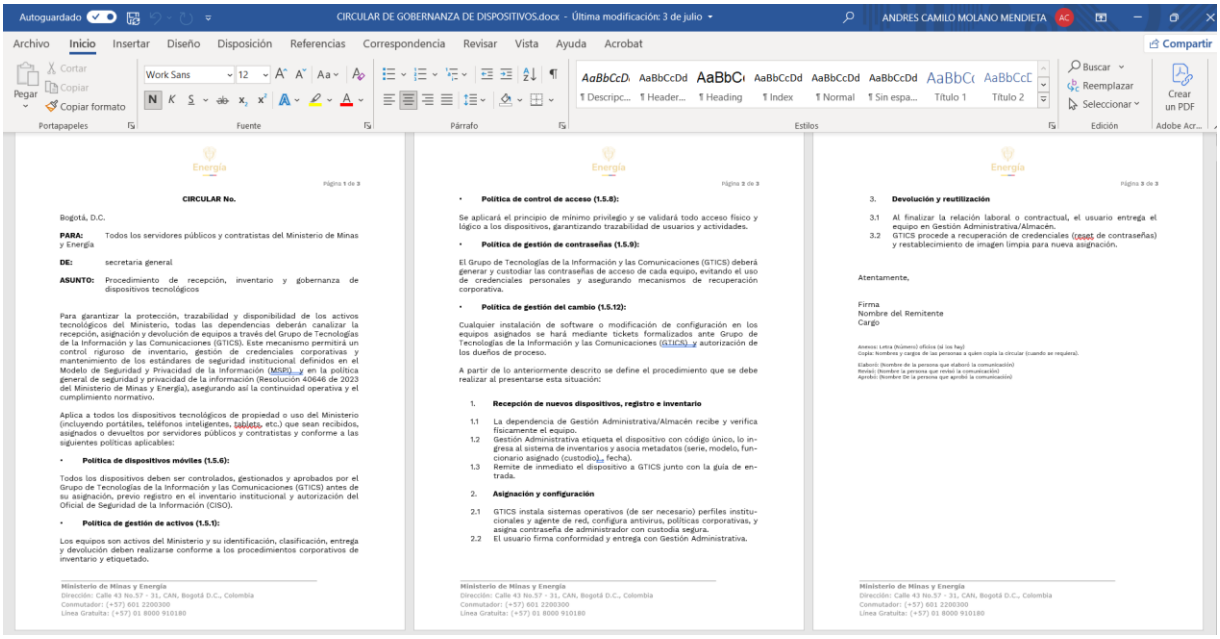


Imagen [22]. Circular estructurada para el manejo y gobernanza de la los dispositivos TI .

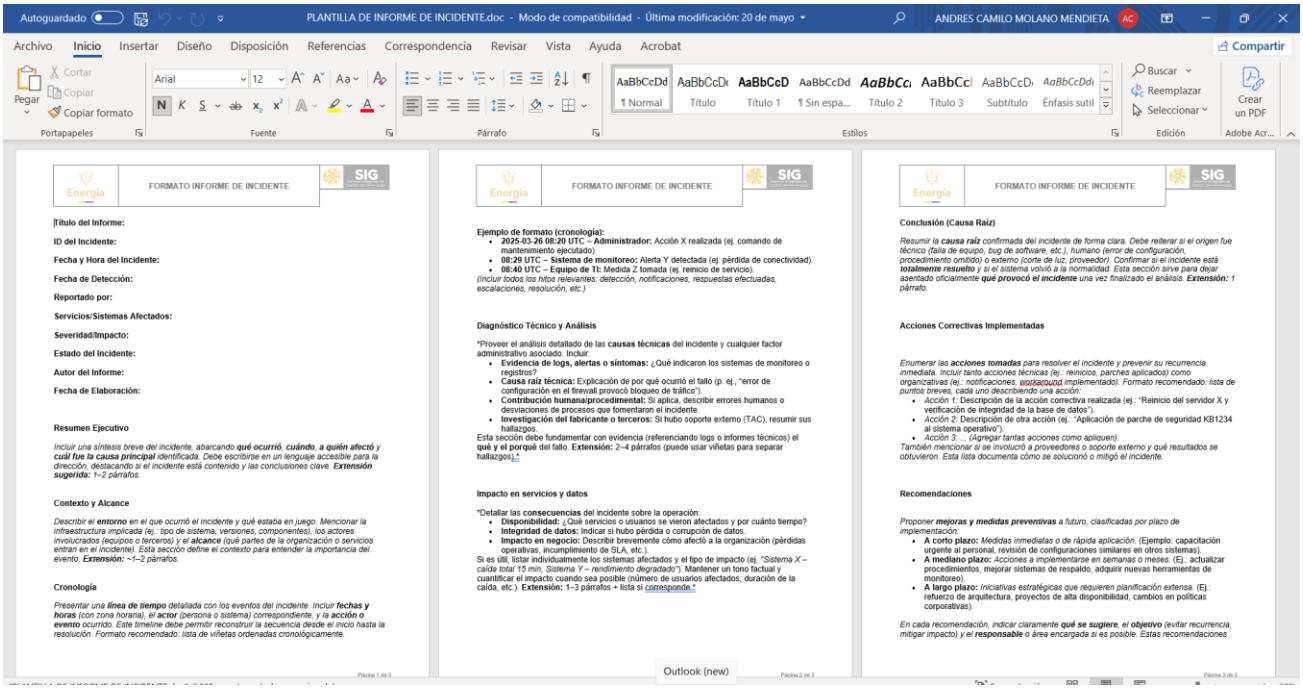


Imagen [23]. Plantilla de informe de gestión de incidentes.

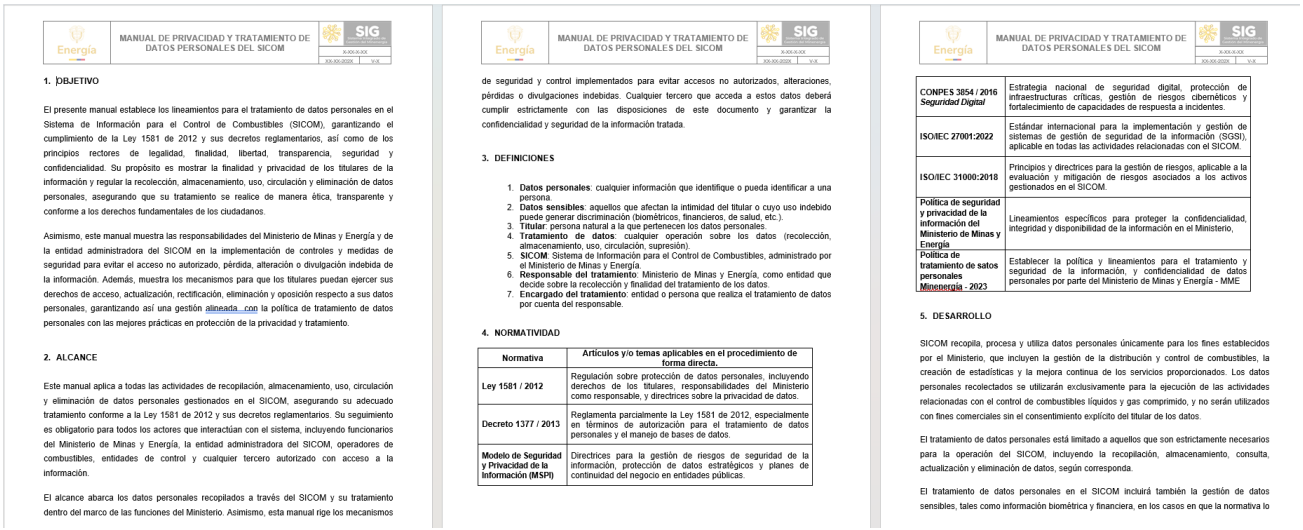
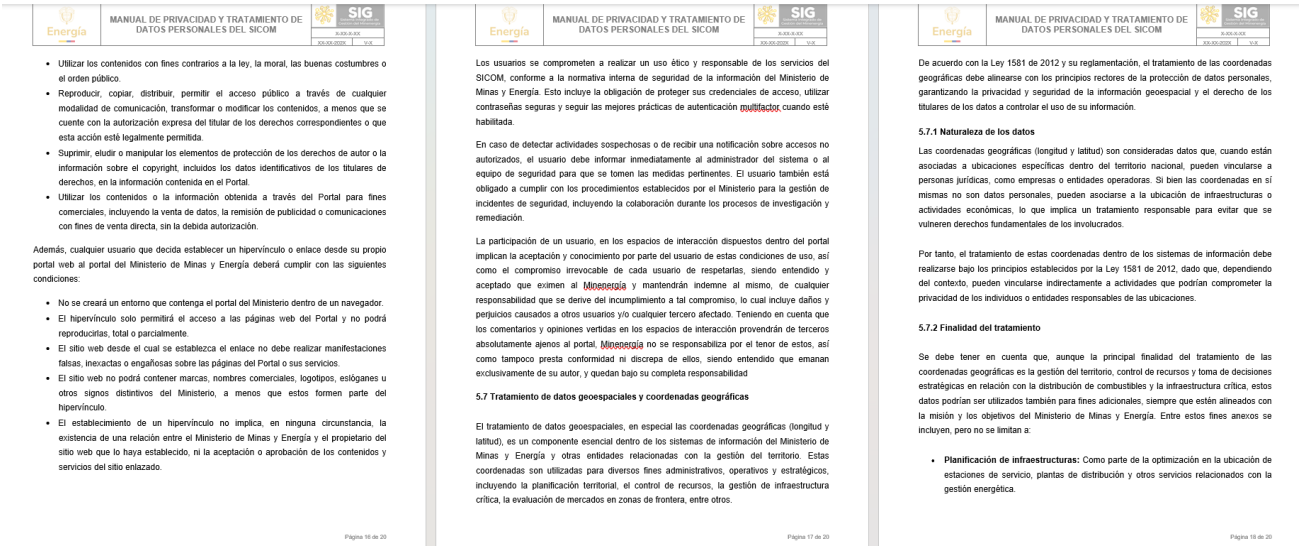


Imagen [24]. Manual de uso y tratamiento de datos personales de SICOM



MANUAL DE PRIVACIDAD Y TRATAMIENTO DE DATOS PERSONALES DEL SICOM

- Utilizar los contenidos con fines contrarios a la ley, la moral, las buenas costumbres o el orden público.
- Reproducir, copiar, distribuir, permitir el acceso público a través de cualquier modalidad de comunicación, transformar o modificar los contenidos, a menos que se cuente con la autorización expresa del titular de los derechos correspondientes o que esta acción esté legalmente permitida.
- Suprimir, eludir o manipular los elementos de protección de los derechos de autor o la información sobre el copyright, incluidos los datos identificativos de los titulares de derechos, en la información contenida en el Portal.
- Utilizar los contenidos o la información obtenida a través del Portal para fines comerciales, incluyendo la venta de datos, la remisión de publicidad o comunicaciones con fines de venta directa, sin la debida autorización.

Además, cualquier usuario que decida establecer un hipervínculo o enlace desde su propio portal web al portal del Ministerio de Minas y Energía deberá cumplir con las siguientes condiciones:

- No se creará un entorno que contenga el portal del Ministerio dentro de un navegador.
- El hipervínculo solo permitirá el acceso a las páginas web del Portal y no podrá reproducirlas, total o parcialmente.
- El sitio web desde el cual se establezca el enlace no debe realizar manifestaciones falsas, inexactas o engañosas sobre las páginas del Portal o sus servicios.
- El sitio web no podrá contener marcas, nombres comerciales, logotipos, eslóganes u otros signos distintivos del Ministerio, a menos que estos formen parte del hipervínculo.
- El establecimiento de un hipervínculo no implica, en ninguna circunstancia, la existencia de una relación entre el Ministerio de Minas y Energía y el propietario del sitio web que lo haya establecido, ni la aceptación o aprobación de los contenidos y servicios del sitio enlazado.

Página 16 de 20

MANUAL DE PRIVACIDAD Y TRATAMIENTO DE DATOS PERSONALES DEL SICOM

Los usuarios se comprometen a realizar un uso ético y responsable de los servicios del SICOM, conforme a la normativa interna de seguridad de la información del Ministerio de Minas y Energía. Esto incluye la obligación de proteger sus credenciales de acceso, utilizar contraseñas seguras y seguir las mejores prácticas de autenticación multifactor cuando esté habilitada.

En caso de detectar actividades sospechosas o de recibir una notificación sobre accesos no autorizados, el usuario debe informar inmediatamente al administrador del sistema o al equipo de seguridad para que se tomen las medidas pertinentes. El usuario también está obligado a cumplir con los procedimientos establecidos por el Ministerio para la gestión de incidentes de seguridad, incluyendo la colaboración durante los procesos de investigación y remediación.

La participación de un usuario, en los espacios de interacción dispuestos dentro del portal implican la aceptación y conocimiento por parte del usuario de estas condiciones de uso, así como el compromiso irrevocable de cada usuario de respetarlas, siendo entendido y aceptado que eximen al Minenergía y mantendrán indemne al mismo, de cualquier responsabilidad que se derive del incumplimiento a tal compromiso, lo cual incluye daños y perjuicios causados a otros usuarios y/o cualquier tercero afectado. Teniendo en cuenta que los comentarios y opiniones vertidas en los espacios de interacción provendrán de terceros absolutamente ajenos al portal, Minenergía no se responsabiliza por el tenor de estos, así como tampoco presta conformidad ni discrepa de ellos, siendo entendido que emanan exclusivamente de su autor, y quedan bajo su completa responsabilidad

5.7 Tratamiento de datos geoespaciales y coordenadas geográficas

El tratamiento de datos geoespaciales, en especial las coordenadas geográficas (longitud y latitud), es un componente esencial dentro de los sistemas de información del Ministerio de Minas y Energía y otras entidades relacionadas con la gestión del territorio. Estas coordenadas son utilizadas para diversos fines administrativos, operativos y estratégicos, incluyendo la planificación territorial, el control de recursos, la gestión de infraestructura crítica, la evaluación de mercados en zonas de frontera, entre otros.

Página 17 de 20

MANUAL DE PRIVACIDAD Y TRATAMIENTO DE DATOS PERSONALES DEL SICOM

De acuerdo con la Ley 1581 de 2012 y su reglamentación, el tratamiento de las coordenadas geográficas debe alinearse con los principios rectores de la protección de datos personales, garantizando la privacidad y seguridad de la información geoespacial y el derecho de los titulares de los datos a controlar el uso de su información.

5.7.1 Naturaleza de los datos

Las coordenadas geográficas (longitud y latitud) son consideradas datos que, cuando están asociadas a ubicaciones específicas dentro del territorio nacional, pueden vincularse a personas jurídicas, como empresas o entidades operadoras. Si bien las coordenadas en sí mismas no son datos personales, pueden asociarse a la ubicación de infraestructuras o actividades económicas, lo que implica un tratamiento responsable para evitar que se vulneren derechos fundamentales de los involucrados.

Por tanto, el tratamiento de estas coordenadas dentro de los sistemas de información debe realizarse bajo los principios establecidos por la Ley 1581 de 2012, dado que, dependiendo del contexto, pueden vincularse indirectamente a actividades que podrían comprometer la privacidad de los individuos o entidades responsables de las ubicaciones.

5.7.2 Finalidad del tratamiento

Se debe tener en cuenta que, aunque la principal finalidad del tratamiento de las coordenadas geográficas es la gestión del territorio, control de recursos y toma de decisiones estratégicas en relación con la distribución de combustibles y la infraestructura crítica, estos datos podrían ser utilizados también para fines adicionales, siempre que estén alineados con la misión y los objetivos del Ministerio de Minas y Energía. Entre estos fines anexos se incluyen, pero no se limitan a:

- **Planificación de infraestructuras:** Como parte de la optimización en la ubicación de estaciones de servicio, plantas de distribución y otros servicios relacionados con la gestión energética.

Página 18 de 20

Imagen [25]. Manual de uso y tratamiento de datos personales de 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

El Ministerio ha definido una hoja de ruta clara con seis grandes proyectos estratégicos para 2025, detallados en la Tabla 4. Estos incluyen la contratación de servicios de hacking ético, la implementación de un CSIRT, el desarrollo de un DRP/BCP, la creación de un SOC y la renovación de firewalls y WAF. Para el tercer trimestre, se ha logrado un avance significativo en el proceso de contratación para cada uno de estos proyectos de inversión, superando la parálisis "precontractual" y avanzando hacia la etapa final de adjudicación e inicio pertinente.

Con esta transición de la planificación a la ejecución, las expectativas para el cuarto trimestre se centran en el inicio tangible de las actividades de implementación y seguimiento. Específicamente, se espera poder realizar el seguimiento de la infraestructura del Centro de Monitoreo Sectorial, comenzar la implementación de los nuevos controles y lineamientos del proyecto MSPI 2025, y ejecutar las pruebas pertinentes en el proyecto de *ethical hacking*, incluyendo un ejercicio profundo de ingeniería social. Este avance representa un punto de inflexión crucial, transformando la estrategia de seguridad de un plan en papel a un programa con proyectos activos y resultados medibles.

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 tercer 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 tercer 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%** (NA/NA)	Sin incidentes
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	**40%** (3/7)	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%** (3/3)	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.

5.2 GESTIÓN DE VULNERABILIDADES.

El tercer trimestre de 2025 marcó un período de transición y fortalecimiento para el ciclo de vida de la gestión de vulnerabilidades. Si bien el proceso formal de seguimiento a través de la herramienta Planner se mantuvo, el foco principal del trimestre se desplazó hacia la consolidación del proceso a raíz de un cambio significativo en los custodios y responsables de los sistemas de información e infraestructura. Esta reestructuración organizacional requirió un esfuerzo concentrado en la capacitación y alineación de los nuevos actores para garantizar la continuidad y eficacia del programa a largo plazo.

Las actividades del trimestre se centraron en capacitar a los nuevos responsables sobre sus roles dentro del flujo de trabajo de gestión de vulnerabilidades. Se llevaron a cabo sesiones intensivas para asegurar que cada custodio comprendiera a cabalidad el procedimiento, desde la notificación inicial hasta el cierre. Se hizo especial hincapié en la importancia de utilizar el formato oficial para documentar las acciones de remediación, la necesidad de adjuntar evidencias claras y suficientes que demuestren la corrección de la brecha, y la obligación de establecer y cumplir rigurosamente los tiempos de respuesta acordados, particularmente para las vulnerabilidades de criticidad alta.

Este enfoque en la capacitación y la adopción del proceso tuvo un impacto directo en las métricas de remediación del trimestre, ya que la prioridad fue asegurar una base de conocimiento sólida en lugar de la ejecución inmediata de correcciones. Conscientes de esta situación, se tomó la decisión estratégica de realizar un ajuste fundamental en la planificación: al inicio del cuarto trimestre se llevará a cabo un nuevo escaneo exhaustivo de vulnerabilidades en toda la infraestructura tecnológica. Esta medida permitirá establecer una nueva línea de base completa y actualizada del estado de seguridad de la entidad.

Este re-escaneo integral servirá como punto de partida para el nuevo ciclo operativo, asegurando que los equipos, ahora debidamente capacitados, trabajen sobre la base de la información más reciente y precisa. La expectativa para el cuarto trimestre es que, con un proceso robustecido y responsabilidades claramente asimiladas, la tasa de remediación de vulnerabilidades, especialmente las críticas, mejore significativamente, demostrando el valor de la inversión en la capacitación y consolidación del proceso realizada durante este período de transición.

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 septiembre de 2025 se llevó a cabo una auditoría interna focalizada en el proceso de Gestión Tecnológica, liderada por la Oficina de Planeación y Gestión y llamada “seguridad de la información y accesibilidad web”. 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 tercer trimestre de 2025 se impartieron tres sesiones de formación dirigidas a fortalecer la cultura de seguridad digital en la entidad. La primera charla se centró en el cifrado de información y la transferencia de archivos confidenciales. La segunda sesión abordó las herramientas emergentes como procesos de ciberdefensa e higiene digital para cada una de las personas. Por último, la tercera charla se enfatizó en la divulgación de la estrategia de seguridad nacional digital de Colombia, aplicable para las entidades públicas.

Análisis Detallado de los Resultados de la Campaña de Phishing

En junio de 2025 se realizó una campaña de phishing de recolección de credenciales. Los resultados, presentados en la Tabla-1, fueron alarmantes: el 15% (231 empleados) envió sus credenciales; el 23% (351) hizo clic en el enlace; y el 55% (832) abrió y leyó el correo electrónico.
Una tasa de envío de credenciales del 15% no es simplemente una "oportunidad de formación"; es una emergencia de máxima prioridad. Esto representa una vulnerabilidad crítica y activa que

proporciona una vía directa para que los atacantes eludan las defensas perimetrales. En este contexto, la ausencia total de cualquier mención a la Autenticación Multifactor (MFA) en todo el informe de 46 páginas es una omisión flagrante y probablemente el control técnico más importante que falta en la arquitectura de seguridad del Ministerio. El 15% de los usuarios ha demostrado estar dispuesto a entregar sus contraseñas a un sitio web fraudulento. Las credenciales robadas son uno de los vectores de acceso inicial más comunes para los ataques de ransomware y las violaciones de datos. El control más eficaz para mitigar el riesgo de credenciales robadas es la MFA. La palabra "MFA" o "multifactor" no aparece en ninguna parte del documento. La respuesta para el T3 debe ser un plan de acción de emergencia de tres frentes: (1) Remediación Inmediata: Los 231 empleados que enviaron sus credenciales deben someterse de inmediato a una nueva formación obligatoria, intensiva e individualizada. (2) Implementación de Control Estratégico: Se debe iniciar con la máxima prioridad un proyecto para desplegar la MFA en todos los accesos remotos, servicios en la nube y aplicaciones internas críticas. (3) Endurecimiento Táctico: Se deben revisar las reglas de la pasarela de seguridad del correo electrónico para mejorar el bloqueo de este tipo de ataques antes de que lleguen a las bandejas de entrada de los usuarios.

Imagen [26]. Capacitación de cifrado MME

Imagen [27]. Capacitación de cifrado MME

Imagen [26]. Capacitación de Estrategia nacional de seguridad digital MME

Imagen [27]. Capacitación de Estrategia nacional de seguridad digital MME

Imagen [28]. Capacitación de Herramientas contra hackers MME

Imagen [29]. Capacitación de Herramientas contra hackers MME

Energía