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

Seguimiento Plan de Tratamiento de Riesgos de Seguridad de la Información – Cuarto 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, 15 de Diciembre de 2025

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

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: jagrajales@minenergia.gov.co
Teléfono: (+57) 6012200300 Ext. 2408

3. OBJETIVO

Documentar el seguimiento y evaluación del Plan de Tratamiento de Riesgos de seguridadde la Información implementado por el Ministerio de Minas y Energía (MINENERGÍA). Este plan, revisado y actualizado más recientemente el 28 de diciembre de 2024, tiene como propósito principal garantizar la integridad, confidencialidad y disponibilidad de los activos de información de la entidad, mediante la mitigación efectiva de riesgos identificados y evaluados previamente.

Desde la adopción del plan, el Grupo de Tecnología de la Información y las Comunicaciones(TIC) ha estado comprometido en reforzar las medidas de seguridad informática y mejorarla resiliencia de las plataformas tecnológicas del Ministerio. Este esfuerzo ha sido esencialen el contexto, donde se han adaptado nuevas modalidades de trabajo que demandan robustez en las estrategias de seguridad de la información, para proteger a la entidad contra posibles vulnerabilidades y amenazas cibernéticas.

Este informe se enfoca en la revisión de las acciones implementadas,evaluando la efectividad de los controles y medidas de mitigación adoptadas. Además, se presenta un análisis de los resultados obtenidos, destacando los logros alcanzados y las áreas que aún requieren atención. El seguimiento constante y la actualización del plan son fundamentales para mantener un nivel de riesgo residual aceptable y asegurar la continuidad operativa del MINENERGÍA frente a los desafíos emergentes en el ámbito de la seguridad de la información.

Por otro lado, la identificación y valoración de riesgos residuales han permitido al Grupo TIC adoptar una metodología proactiva basada en la "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6", emitida por el DAFP. Estametodología ha facilitado la implementación de controles más precisos y efectivos, ajustados a las necesidades específicas del Ministerio. Con este seguimiento, se busca reducir vulnerabilidades identificadas y mejorar los procesos de seguridad, garantizando laprotección de la información sensible gestionada por el MINENERGÍA.

4. Plan de tratamiento de riesgos

4.1 Valoración riesgo residual.

la valoración del riesgo residual es una etapa clave para determinar la eficacia de los controles implementados y garantizar que los riesgos se mantengan dentro de niveles tolerables para el Ministerio de Minas y Energía.

La valoración del riesgo residual para 2025 incorporará un análisis más granular de los controles existentes, midiendo no solo su implementación, sino también su efectividad en reducir los riesgos inherentes. Este análisis incluirá métricas claras, como el porcentaje de reducción del riesgo tras la implementación de los controles, y priorizará aquellos riesgos con mayor impacto sobre los sistemas críticos, como plataformas tecnológicas, bases de datos estratégicas y servicios en la nube.

Dicho lo anterior es importante revisar los resultados del plan de tratamiento de riesgos de la entidad para el año 2024, de esta forma tenemos las siguientes conclusiones:

Tabla 1

Logros de cada uno de los riesgos del "plan de tratamiento de riesgos 2024"

Riesgo	Conclusión
R5 - Implementación de Código Seguro	Se lograron avances en el anexo de las secciones de lineamientos de código seguro en la metodología de desarrollo de software del ministerio, incluyendo la creación de un checklist y buenas prácticas. El equipo de desarrollo se encuentra en etapa 1 de autodiagnóstico en cada uno de los sistemas de información, software y aplicaciones para determinar fallas y oportunidades de mejora y aplicabilidad de código seguro en la epata 2 vigencia 2025.
R11 - Auditoría de los Sistemas de Información	Se habilitaron módulos de auditoría en 15 sistemas críticos, con procesos de monitoreo y control. Se requiere formalizar un procedimiento estandarizado para su aplicación y una política que determine la importancia de esta característica en las sistemas de información, software y aplicaciones que así lo requieran.
R14 - Gestión de Backups	Se ejecutaron con éxito los procesos de backup planificados, detectándose oportunidades de mejora en la automatización y documentación. Se destaca la que herramienta para dicho fin ArcServ se encuentra funcionando al 80% de su capacidad y presentó fallas al momento de realizar tarea, de manera que se debe evaluar si es prescindible seguirla

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

Riesgo	Conclusión
	usando, actualizarla o reemplazarla.
R16 - Pruebas de Continuidad del Negocio	Se avanzó en la actualización del DRP con simulacros controlados (reinicio de servidores y funcionamiento del centro de datos alterno) , esto implica ante un escenario de crisis la entidad puede restablecer sus sistemas de información en condiciones óptimas a nivel técnico, sin embargo, existen más escenarios que deben nutrir el plan de recuperación ante desastres.
R18 - Soluciones Criptográficas	Se implementaron mecanismos de cifrado de información crítica, incluyendo un manual de cifrado y la adopción de herramientas destinadas para este fin.
R22 - Contratación de Infraestructura IT	Se cerraron contratos clave para fortalecer la infraestructura tecnológica, estableciendo lineamientos para futuras adquisiciones alineadas con la estrategia de seguridad.

Con base en los resultados obtenidos durante la vigencia 2024 (tabla anterior) , se concluye que se aplicaron diversos controles y medidas de mitigación para abordar los riesgos identificados en el Plan de Tratamiento de Riesgos de Seguridad de la Información del Ministerio de Minas y Energía. Sin embargo, no todos los riesgos fueron completamente mitigados, ya que la naturaleza dinámica del entorno digital implica la presencia continua de amenazas latentes que requieren un monitoreo y ajuste constante. Además, algunos controles y actividades planificadas durante el periodo no se ejecutaron de manera óptima, lo que generó la necesidad de continuar su tratamiento en la vigencia 2025.

A pesar de los esfuerzos realizados, se identificaron riesgos que presentan una valoración residual, lo que implica que ciertos controles deben mantenerse y reforzarse de forma continua para garantizar un nivel adecuado de seguridad. Es fundamental reconocer que la seguridad de la información es un proceso dinámico, donde la evolución de amenazas y vulnerabilidades exige la implementación de estrategias de mitigación adaptativas. Durante el 2024, se lograron avances importantes en áreas como la gestión de backups, auditoría de sistemas de información, estructuración de código seguro y fortalecimiento de la infraestructura tecnológica; sin embargo, algunos procesos requieren ajustes adicionales para su completa efectividad.

Para la vigencia 2025, se establecerán planes de acción específicos para abordar los riesgos residuales y completar las actividades pendientes de ejecución. Esto incluirá la optimización de los procedimientos de auditoría, la automatización de procesos de respaldo y la formalización de controles de desarrollo seguro. La continuidad de estos esfuerzos garantizará la mejora constante de la postura de seguridad del Ministerio, minimizando las probabilidades de materialización de amenazas y asegurando la disponibilidad, integridad y confidencialidad de los activos de información críticos.

Dicho lo anterior se define los siguientes riesgos que contemplan un riesgo residual y nuevos

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

riesgos a trabajar en la vigencia 2025 :

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.

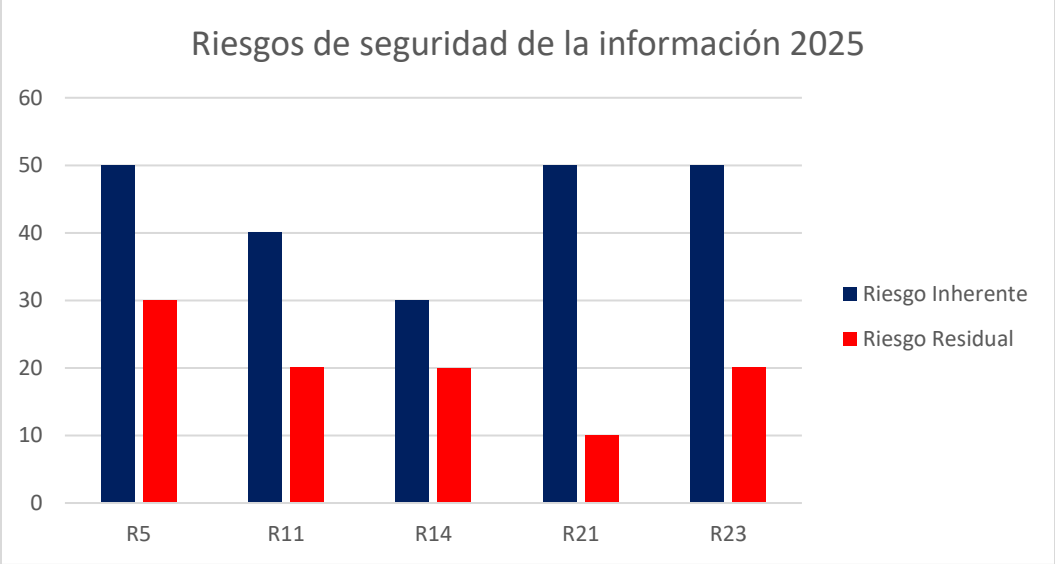
Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

	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.
R23	Procedimiento Gestión de Continuidad y Recuperación de los Servicios de Informática y Comunicaciones. Ausencia de DRP actualizado. **Actividades necesarias:** 1. Evaluar la infraestructura tecnológica actual y actualizar el DRP con base en las mejores prácticas y estándares

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

	2. Incorporar la clasificación actualizada de los activos de información, identificando aquellos críticos para la operatividad del Ministerio. 3. Ejecutar pruebas de recuperación controladas en entornos de prueba que simulen diferentes escenarios de fallas, como pérdida de datos, ataques cibernéticos o fallos de infraestructura. 4. Evaluar la efectividad de los procedimientos definidos en el DRP y realizar ajustes en función de los resultados obtenidos.

Ilustración 1 - Comparativo Riesgo Residual e Inherente por número de riesgo.



Fuente: Grupo TICS

La ilustración anterior presenta una evaluación detallada de los riesgos de seguridad de la información, la barra de color azul representa el riesgo inherente, que corresponde al nivel de riesgo existente antes de la aplicación de cualquier control o medida de mitigación. Este riesgo refleja tanto el impacto potencial como la probabilidad de que ocurra un evento adverso si no se implementan acciones preventivas o correctivas. Es el punto de partida sobre el cual se establecen las estrategias de gestión de riesgos del Ministerio.

Por otro lado, la barra de color rojo representa el riesgo residual, que corresponde al nivel de riesgo que permanece después de la implementación de controles en la vigencia 2024. Aunque se han aplicado medidas de seguridad para mitigar los riesgos, algunos no pueden eliminarse por completo debido a la naturaleza cambiante del entorno de amenazas cibernéticas y a la evolución constante de los activos tecnológicos. Además, ciertos riesgos forman parte de

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

procesos continuos de mejora y actualización, en función de lineamientos normativos, tecnológicos y operativos que requieren ajustes periódicos para mantener la seguridad y resiliencia de la información.

El análisis comparativo entre los riesgos inherentes y residuales demuestra la efectividad de los controles aplicados y permite identificar áreas de oportunidad para la vigencia 2025, con el fin de reforzar la postura de seguridad del Ministerio y asegurar la protección de la información crítica frente a amenazas emergentes.

4.2 Vulnerabilidades a eliminar de los riesgos que requieren tratamiento

4.2.1 Seguimiento del plan de gestión:

En cumplimento con el plan de tratamiento de riesgos de seguridad de la información se tiene el siguiente resumen que indica el roadmap o hoja de ruta llevado a cabo por actividad, la frecuencia de cada de una de las actividades puede variar de informe mensual a trimestral de manera que se hace una recopilación de los mismos en la siguientes tablas. Acciones de seguimiento y cumplimento para cada uno de los riesgos mapeados para el primer trimestre

Tabla 3
Reporte primer trimestre plan de tratamientos de riesgos de seguridad de la información- actividades realizadas.

No	Reporte primer Trimestre
R5	Se mantiene el control de la mitigación en un alto porcentaje. Esto se logró gracias a la implementación de la metodología de código seguro, la creación de un listado de requerimientos mínimos para el desarrollo de software (incluyendo buenas prácticas, retest, QA, pruebas aleatorias de vulnerabilidades conocidas, entre otros), y la adopción de nuevas prácticas de desarrollo enfocadas en Opensource en 4 aplicaciones nuevas para la entidad, dejando un aprendizaje continuo, en despliegue, operación y puesta en marcha, con la meta de obtener retroalimentación de brechas de seguridad que se puedan ir evidenciando en operación y uso por parte de los usuarios finales.
R11	Se llevaron a cabo auditorías adicionales a los logs de los sistemas de información para fortalecer el monitoreo y control, generando informes trimestrales. Se espera que en vigencia del segundo trimestre se implementen los Logs para los sistemas de información que estén manejado información reservada y clasificada, de manera que se establecerá una mesa de trabajo con las partes interesadas para evaluar que SI son necesarios para dicha actividad, así mismo determinar un procedimiento estandarizado para la implementación de módulos de auditoría.

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

R14	Durante el primer trimestre se llevaron a cabo actividades clave para optimizar el sistema de respaldos de la organización, utilizando la herramienta Arcserve ASBU y UDP Backup. Se consolidaron 230 servidores respaldados a disco, mejorando la cobertura y los tiempos de recuperación. Paralelamente, se realizó una depuración exhaustiva de los puntos de restauración históricos con el proveedor SVAIT, liberando 20TB de espacio en almacenamiento y mejorando el rendimiento del sistema. Esta liberación permitió relanzar los respaldos de correos y bases de datos que estaban represados. Además, se planificó un Backup Full Granular a Cinta para marzo de 2025, como parte de una estrategia de seguridad a largo plazo. Estas acciones, junto con la implementación de métricas clave como tasas de éxito/falla, capacidad de almacenamiento disponible y tiempos de recuperación, permitirán evaluar la efectividad de la herramienta y determinar si se debe continuar con Arcserve o considerar su reemplazo.
R21	Se realiza mesa de trabajo con el grupo de gestión documental , oficina de planeación y grupo TICS con el objetivo de modificar adecuadamente la matriz de activos de información, alineando un único instrumento que funcione de manera automatizada para todas las áreas de la entidad ; Finalización del instrumento a la espera de reunión con el área de comunicaciones y OAJ , para iniciar capacitación a los lideres SIG; Unificación de información ya diligenciada en el nuevo instrumento, recoger de del instrumento del índice de información clasificada y reservada la alineación con los objetivos estratégicos de la entidad, con base a estas actividades se proyecta el diligenciamiento adecuado de los BIA y BCP para actualizarlos en vigencia.
R23	1. En el primer trimestre del año 2025 se avanzó en la construcción de la ficha técnica para "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." junto con la documentación necesaria para realizar el sondeo de mercado de este proceso. 2. Se han revisado varias herramientas de replicación entre centro de datos junto con su funcionamiento y características para generar la documentacion de anexo tecnico y generar proceso de estudios previos y sondeo de mercado durante el segundo semestre. 3. Se revisaron diversas alternativas de servicios de “colocation” con el objetivo de trasladar el datacenter alterno, garantizando condiciones de integridad, cumplimiento normativo y las facilidades técnicas necesarias para su correcto funcionamiento. Como parte de esta actividad, se realizaron visitas técnicas a diferentes proveedores potenciales, entre ellos: Nebula/Hostname, Ilkary, Internexa, Cotel y Tigo. Adicionalmente, se adelantó la actualización del inventario y del valor en libros del datacenter alterno, como parte del proceso de planificación y toma de decisiones.

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

Tabla 4

Reporte segundo trimestre plan de tratamientos de riesgos de seguridad de la información- actividades realizadas.

No	Reporte Segundo Trimestre
R5	Código y desarrollo seguro: Durante el segundo trimestre de 2025, se reforzó el control sobre la seguridad en el ciclo de vida del software mediante la integración de pruebas y revisiones automatizadas en GitLab. Se desplegaron pipelines de CI/CD que incorporan validaciones de estilo de código, chequeos de dependencias y pruebas de QA, garantizando la detección temprana de vulnerabilidades conocidas antes del despliegue . Paralelamente, se estableció un repositorio privado de imágenes Docker en Nexus, donde todas las builds son escaneadas y versionadas, lo cual asegura un entorno de ejecución confiable y auditable, alineado con la política de soberanía digital y reduciendo la exposición a componentes inseguros. Adicionalmente, se produjo la liberación de dos nuevas aplicaciones (un sistema de asistencias en Laravel y una ventanilla única en Python + Vue.js) bajo este esquema de desarrollo seguro. Cada proyecto incorporó desde su inicio el listado de requerimientos mínimos de seguridad (buenas prácticas, retest de código y pruebas aleatorias de vulnerabilidades), permitiendo no sólo un despliegue ágil sino también un aprendizaje continuo en operación.
R11	Durante el segundo trimestre de 2025 se avanzó en la identificación y configuración de los módulos de auditoría (logs) en los diferentes sistemas de información bajo la gobernabilidad del Ministerio. Se levantó un inventario detallado que distingue entre los SI que ya cuentan con funcionalidad de auditoría (como el Buzón de Integridad y Transparencia, SISEG, el módulo “site-history” en Wagtail para el portal web, la intranet y EITI Colombia) y aquellos que operan únicamente en modo de consulta, sujetándose a evaluación técnica para determinar su viabilidad de incorporación del rol de auditor. Aunque en este segundo trimestre no se realizaron actualizaciones a los módulos existentes, se estableció una hoja de ruta para 2025 que contempla: 1. Documentar en el catálogo de aplicaciones los SI que no incorporarán auditoría, incluyendo sus argumentos funcionales y técnicos. 2. Formalizar un procedimiento estándar de implementación de módulos de auditoría con herramientas ágiles y alineadas a las políticas de seguridad y privacidad del Ministerio, de modo que a partir del tercer trimestre se inicie la actualización y despliegue de dichas capacidades

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

R14	Evaluación y simulacro de procesos de respaldo: Durante el segundo trimestre de 2025 se avanzó en la consolidación del appliance Arcserve UDP, respaldando un total de 204 servidores contra disco. Como parte de esta fase, se depuraron los puntos de restauración históricos, liberando 26.3 TB en la partición x:\UDPData1 —incrementando el espacio libre de 1.5 TB a 26.8 TB— lo que permitió reactivar inmediatamente los respaldos de los buzones de correo y las bases de datos que estaban en cola. Además, tras finalizar la depuración, se inició el Backup Full granular a cinta el 6 de junio. Hasta la fecha se han procesado 11.6 TB de los 58.5 TB totales, completando aproximadamente el 20 % del volumen en 18 días. Con base en este ritmo de procesamiento, se estima que el trabajo concluirá en cerca de 94 días, garantizando así un ciclo de respaldo robusto y escalable tanto en disco como en cinta para el Ministerio.
R21	Cronograma para la gestión de activos de información y planes de continuidad: En el segundo trimestre de 2025 se completó la implementación del instrumento único de gestión de activos de información, consolidando en una primera fase los catálogos de licenciamiento, sistemas de información e infraestructura elaborados junto al equipo de Arquitectura Empresarial, de esta manera, se puede continuar con la capacitación a los lideres SIG de la entidad para el diligenciamiento adecuado y paralelo a esto continuar con la estructuración de los BCP y BIA correspondientes. No obstante, con la entrada en vigor del nuevo Modelo de Seguridad y Privacidad de la Información (MSPI), se identificó la necesidad de incorporar un módulo específico para la identificación de infraestructura crítica cibernética. Por ello, el instrumento está en proceso de revisión y ajuste durante el tercer trimestre, de modo que, una vez actualizado, permita un solo ejercicio integrado de valoración de activos y continuidad operacional acorde con los lineamientos del MSPI.
R23	En el segundo trimestre, se avanzó en el diseño técnico de la solución y se inició el proceso contractual para la adquisición de una herramienta de respaldo con almacenamiento inmutable y replicación automática, así como el traslado del centro de datos alterno a una infraestructura externa que cumpla con los requisitos del Ministerio. Adicionalmente, se están ejecutando mantenimientos físicos y lógicos a la infraestructura tecnológica, y se ha elaborado un anexo técnico en proceso de ajuste, en el marco de una estrategia de implementación estructurada que ha superado las etapas de diagnóstico y planificación, encontrándose actualmente en la fase de perfeccionamiento contractual. Estas acciones permiten mitigar de forma progresiva el riesgo, fortaleciendo la capacidad institucional de recuperación y continuidad ante eventos críticos.

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

Tabla 5

Reporte Tercer trimestre plan de tratamientos de riesgos de seguridad de la información- actividades realizadas.

No	Reporte Tercer Trimestre
R5	En le tercer trimeste el equipo de desarollo 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. Así mismo, se encuentra en proceso de actualización el documento "Manual – Metodología y Arquitectura de Referencia para el Desarrollo de Sistemas de Información", incorporando en esta versión los lineamientos relacionados con la estrategia DevOps y la implementación de prácticas CI/CD. Estas acciones hacen parte del proceso de fortalecimiento continuo de la metodología de desarrollo y de la adopción de controles automatizados de seguridad, con el propósito de garantizar la integridad, disponibilidad y confidencialidad del software desarrollado por la entidad

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

R11	Durante el tercer trimestre de 2025 se consolidó el procedimiento para habilitar y configurar módulos de auditoría (logs) en los SI bajo gobernabilidad del Ministerio, alineado con las políticas institucionales de seguridad, datos personales, continuidad y recuperación ante desastres. Se precisó que no todos los SI requieren o permiten auditoría, por lo que se profundizó en el diagnóstico técnico-funcional para diferenciar: (a) sistemas con módulo y funcionalidad de auditoría activa (GLPI/ServiceDesk, Buzón de Integridad y Transparencia, SISEG, Encuesta de Medición y Cultura Organizacional, y VUT en ambiente de pruebas con consultas, filtros y comparación de cambios), y (b) sistemas en modo consulta o de interoperabilidad sujetos a evaluación de viabilidad. Se avanzó en el mapeo y trazabilidad (tipo de software, versionamiento, licenciamiento y vigencia de soporte) para decidir la inclusión del rol auditor solo donde aporte valor y sea técnicamente posible.
R14	Evaluación y simulacro de procesos de respaldo: Durante el tercer trimestre de 2025 se avanzó en la consolidación del appliance Arcserve UDP: 1. Se continua con la consolidación de la herramienta del appliance backup arcserve UDP a disco con 169 Servidores respaldados y un pendiente en curso de 52 Servidores virtuales, los cuales se han venido migrando desde el VCenter HyperFlex CISCO con IP 172 .17.1.115 hacia el nuevo Venter DELL. 2. Se continua con la depuración de almacenamiento en disco de la partición X:\UDPData1 y a hoy se han depurado 2.9TB, pasando de 22 a 24.9TB libres en esta partición XXXXX 3. El día 19 de septiembre, por solicitud del Ing. Jaider Ospina se solicitó soporte para la restauración del servidor SRVAPLPRDRAIS con IP 172.17.X.XXX, a la versión del 1XXX de septiembre a las XXX a.m. lo anterior tiene por objetivo revertir un procedimiento técnico realizado en la aplicación y a su vez, realizar un ejercicio de recuperación que permita validar el RTO y el RPO.
R21	Alineación de la matriz de activos de información con el nuevo modelo del MSPI 2025 - circular y puesta en marcha de la metodología de diligenciamiento que promueve información de delegados, capacitación y retroalimentación. En el tercer trimestre de 2025, se estableció ajustes de a la plantilla de los BCP Y BIAS para la entidad conforme a los nuevos lineamientos Sugerencias del MSPI 2025 Formulación de circular interna desde secretaria general (40028 del 24 de septiembre del 2025) para envió de información de delegados de las diferentes de dependencias e inicio de cronograma del diligenciamiento acorde.

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

R23	En el tercer trimestre, se finaliza el proceso de legalización y adjudicación del proyecto de inversión del centro de monitorio sectorial (CMS) en donde se implementa el CDA para la entidad , de manera que se pueda desplegar de forma más robusta una solución de DRP adecuada además de una capa de seguridad mas elevada en la estrategia de seguridad en profundidad con el componente de NOC/SOC dedicado a la infraestructura. Además de esto se establece junto el riesgo R21 la identificación de los activos de información críticos de la entidad ya que se han actualizado los procesos.

Tabla 6

Reporte Cuarto trimestre plan de tratamientos de riesgos de seguridad de la información- actividades realizadas.

No	Reporte Cuarto Trimestre
R5	En el cuarto trimestre de 2025, el equipo de desarrollo culminó la remediación de las vulnerabilidades de alta prioridad que habían quedado pendientes en evaluaciones anteriores, alcanzando así un 100% de cierre de hallazgos críticos identificados durante el año. Adicionalmente, se llevó a cabo una nueva ronda de pruebas de seguridad sobre aplicaciones recientemente implementadas, incluyendo una segunda auditoría de código y pruebas de penetración controladas en el sistema Ventanilla Única de Trámites ya desplegado. Los resultados de estas evaluaciones mostraron solo hallazgos de criticidad baja, los cuales fueron documentados y se encuentran en proceso de corrección dentro de los ciclos de desarrollo. Por otro lado, se finalizó la actualización del "Manual de Metodología y Arquitectura de Referencia para el Desarrollo de Sistemas de Información" para incluir formalmente las prácticas DevOps y de desarrollo seguro establecidas durante 2025. De esta manera, al cierre del año la entidad cuenta con un SDLC fortalecido y estandarizado, complementado por herramientas automatizadas en sus pipelines, lo que reduce significativamente el riesgo de introducir vulnerabilidades en el software institucional. Estas prácticas quedan institucionalizadas de cara a 2026, garantizando que la seguridad por diseño siga siendo un pilar en el desarrollo de nuevos sistemas.
R11	Durante el cuarto trimestre de 2025, tras la formalización del procedimiento estándar de auditoría en el trimestre anterior, se emprendió la implementación ampliada de módulos de logging en otros sistemas críticos de la entidad. Se priorizaron aquellas aplicaciones identificadas como viables durante el diagnóstico (por ejemplo, sistemas que manejan datos reservados pero que carecían de auditoría). Al finalizar el trimestre, se integraron módulos de auditoría en 5 sistemas adicionales, elevando el total a 20 sistemas con esta capacidad operativa. Paralelamente, se emitió una directriz interna que establece la obligatoriedad de incorporar funciones de auditoría en el desarrollo de nuevos sistemas de información, asegurando la continuidad de esta práctica. También se definió un plan

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

	de monitoreo periódico de logs: a partir de 2026, el Grupo de Seguridad de la Información realizará revisiones trimestrales de los registros generados, con el fin de detectar y atender proactivamente eventos anómalos. Con estas acciones, el riesgo asociado a la falta de auditoría en los sistemas se ha reducido y se ha fortalecido la cultura de monitoreo continuo dentro de la institución.
R14	En el cuarto trimestre de 2025, se completó la migración de la totalidad de los servidores pendientes al nuevo entorno de respaldo, consolidando así el alcance del *appliance* Arcserve UDP en la infraestructura del Ministerio. Adicionalmente, tras la adjudicación del nuevo contrato de solución de respaldos (con almacenamiento inmutable y replicación automática) mencionada en trimestres anteriores, se dio inicio a su implementación. Durante este trimestre, el proveedor suministró la plataforma requerida y el equipo técnico del Ministerio realizó las configuraciones iniciales y pruebas piloto de integridad de datos, preparando el terreno para un cambio de plataforma de backups en 2026. Asimismo, con base en las lecciones aprendidas de los simulacros de restauración efectuados en el tercer trimestre, se actualizaron los procedimientos operativos estándar para la recuperación ante desastres, documentando tiempos reales de RTO/RPO y recomendaciones para optimizar dichos indicadores. Aunque la herramienta Arcserve continuó operativa durante este período, sus limitaciones identificadas (uso al 80% de capacidad y fallas esporádicas) están en vía de subsanarse mediante la transición planificada a la nueva solución de respaldo. En resumen, al cierre de 2025 la organización cuenta con un sistema de backups más depurado y con un plan en marcha para modernizar su plataforma de respaldo, lo que en conjunto reduce el riesgo de pérdidas de datos significativas. 1. Se continua con la depuración de almacenamiento en disco de la partición X:\UDPData1 y a hoy se han depurado 2.9TB, pasando de 32.5 a 37TB libres en esta partición XXXXX .
R21	En el cuarto trimestre de 2025 se llevó a cabo la ejecución del plan de clasificación de activos de información con la participación activa de las dependencias. En total se impartieron 4 jornadas de capacitación especializadas: 2 dirigidas a la gestión de inventarios de activos de información y 2 enfocadas en la elaboración de BIA y BCP, con el fin de fortalecer las capacidades de los funcionarios responsables en cada área. Como resultado de la Circular 40028 (septiembre de 2025), fueron designados enlaces de información en 20 dependencias de la entidad, quienes actuaron como puntos focales para coordinar el diligenciamiento de la matriz de activos. Se estableció el 12 de diciembre de 2025 como fecha límite para el primer ejercicio de levantamiento del inventario de activos; a dicha fecha, 9 dependencias (45% del total) habían entregado su matriz de activos de información completa, cumpliendo con la responsabilidad asignada. Este primer ciclo de recopilación

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

	sirvió para identificar desafíos y buenas prácticas, que serán tenidos en cuenta en las siguientes fases. Adicionalmente, se definió un cronograma para 2026 que incluye nuevas capacitaciones de refuerzo y fechas de corte trimestrales para que las dependencias restantes completen y mantengan actualizado el inventario de sus activos de información. Estos avances del cuarto trimestre representan un paso significativo en la actualización del inventario institucional de activos, sentando las bases para la posterior valoración de impacto (BIA) y la formulación/ajuste de los planes de continuidad (BCP) durante 2026..
R23	Durante el cuarto trimestre de 2025, tras la adjudicación del proyecto del Centro de Monitoreo Sectorial (CMS) en el trimestre anterior, se iniciaron las actividades de implementación de las mejoras planificadas en materia de continuidad del negocio. En este periodo, se avanzó en la configuración inicial de la nueva solución de respaldo adquirida, la cual ofrece funcionalidad de almacenamiento inmutable y replicación automática entre centros de datos. El equipo de TI, con el apoyo del proveedor, realizó la instalación de los componentes base en un entorno controlado y llevó a cabo pruebas preliminares de copia y restauración de datos, verificando la operatividad de la herramienta. Paralelamente, se concretaron las gestiones administrativas y técnicas para el traslado del Centro de Datos Alterno a la infraestructura externa seleccionada: se firmó el acuerdo de nivel de servicio con el proveedor de *hosting* y se elaboró un plan detallado de migración, programado para ejecutarse a inicios de 2026, garantizando que el nuevo sitio cumpla con los requerimientos de seguridad y continuidad establecidos. En cuanto a la documentación, durante este trimestre se puso en marcha la actualización del Plan de Recuperación ante Desastres (DRP) de la entidad.

Para cada una estas actividades se tienen el siguiente proceso detallado de resultados:

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.

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

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

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

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.

Avances cuarto trimestre:

el equipo de desarrollo culminó la remediación de las vulnerabilidades de alta prioridad que habían quedado pendientes en evaluaciones anteriores, alcanzando así un 100% de cierre de hallazgos críticos identificados durante el año.

Adicionalmente, se llevó a cabo una nueva ronda de pruebas de seguridad sobre aplicaciones recientemente implementadas, incluyendo una segunda auditoría de código y pruebas de penetración controladas en el sistema Ventanilla Única de Trámites ya desplegado. Los resultados de estas evaluaciones mostraron solo hallazgos de criticidad baja, los cuales fueron documentados y se encuentran en proceso de corrección dentro de los ciclos de desarrollo.

Por otro lado, se finalizó la actualización del “Manual de Metodología y Arquitectura de Referencia para el Desarrollo de Sistemas de Información” para incluir formalmente las prácticas DevOps y de desarrollo seguro establecidas durante 2025. De esta manera, al cierre del año la

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

entidad cuenta con un SDLC fortalecido y estandarizado, complementado por herramientas automatizadas en sus pipelines, lo que reduce significativamente el riesgo de introducir vulnerabilidades en el software institucional. Estas prácticas quedan institucionalizadas de cara a 2026, garantizando que la seguridad por diseño siga siendo un pilar en el desarrollo de nuevos sistemas

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 tercer 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 Cuarto 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,

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

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.

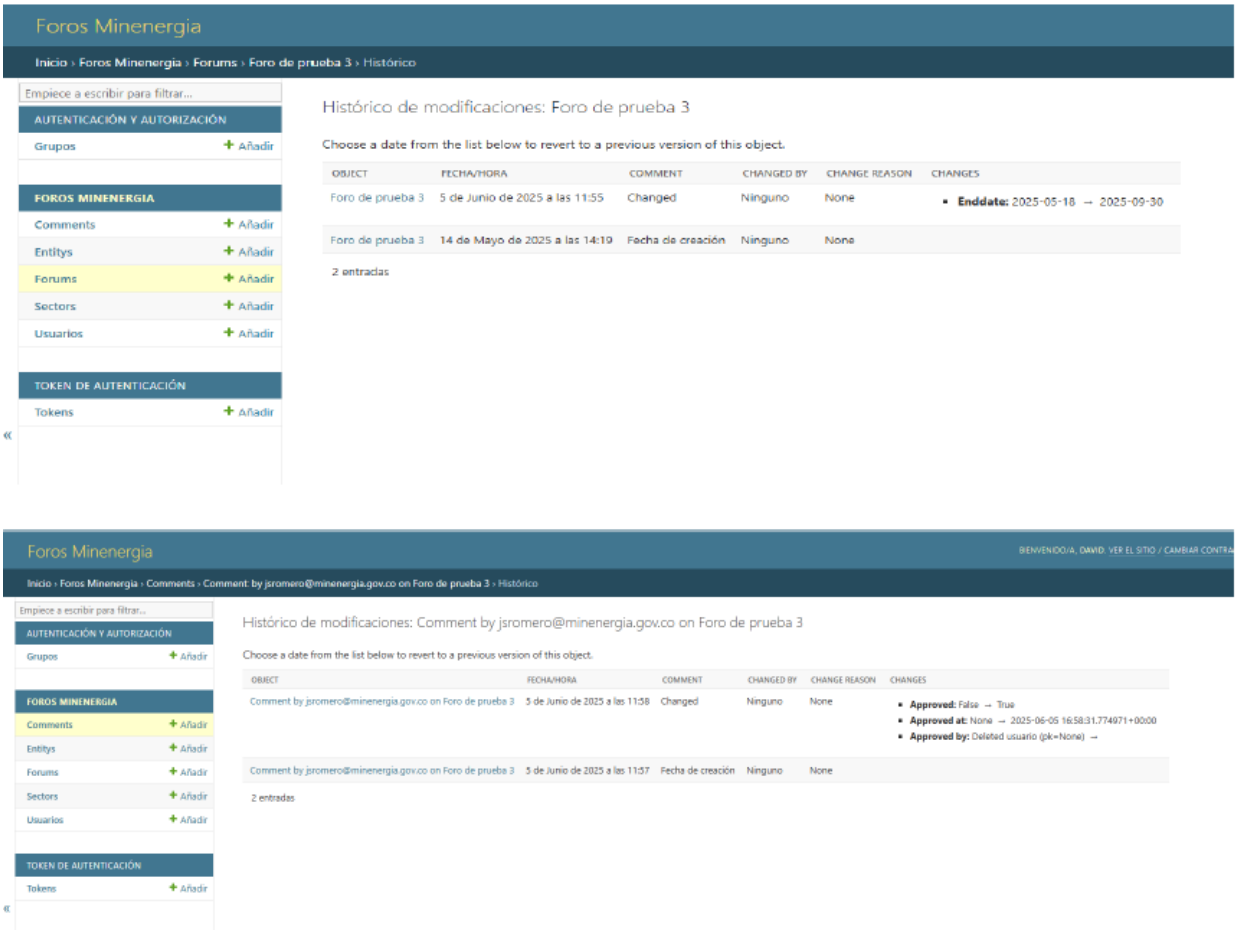


Imagen 1 . Modulo de auditoria Sección servicio al ciudadano – foros

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

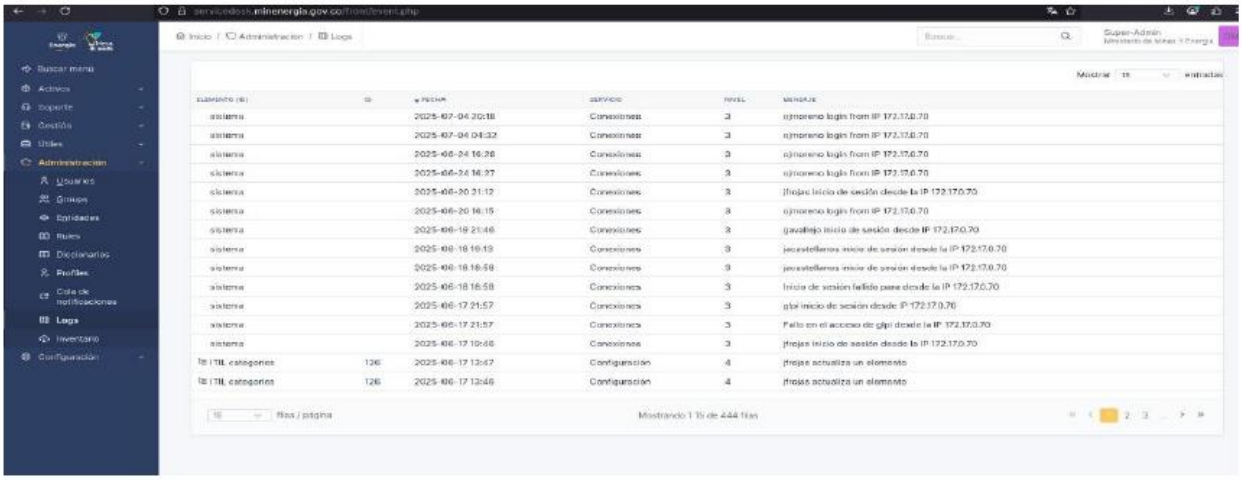
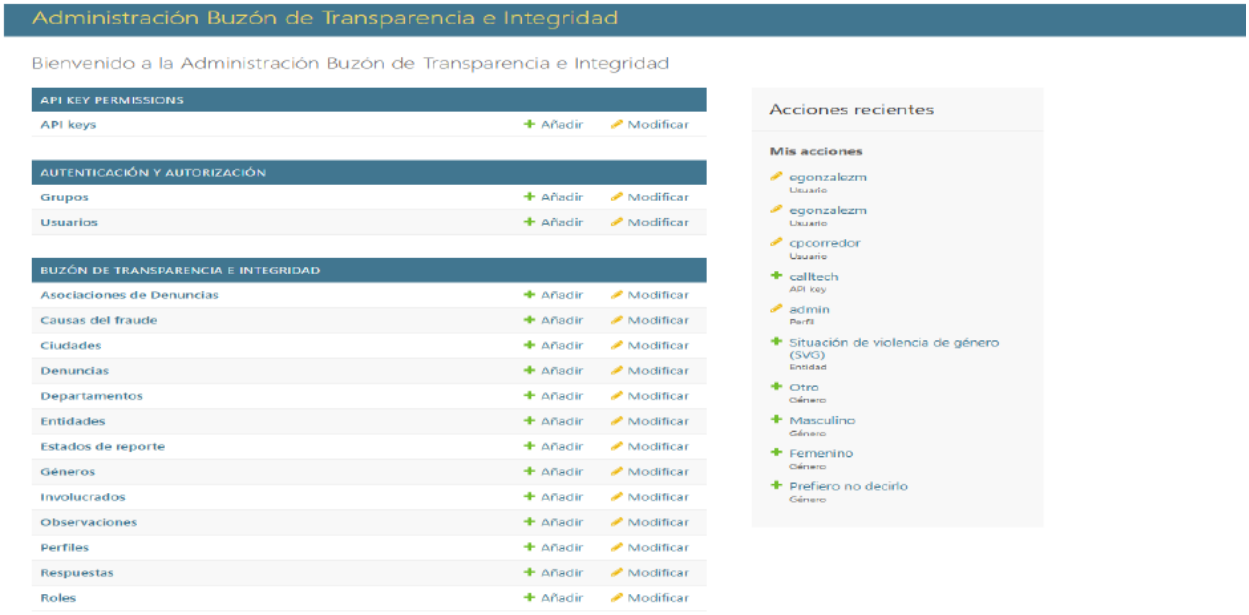


Imagen 2. Modulo de auditoria Gestión de servicios de código abierto- Servicedesk GLPI

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



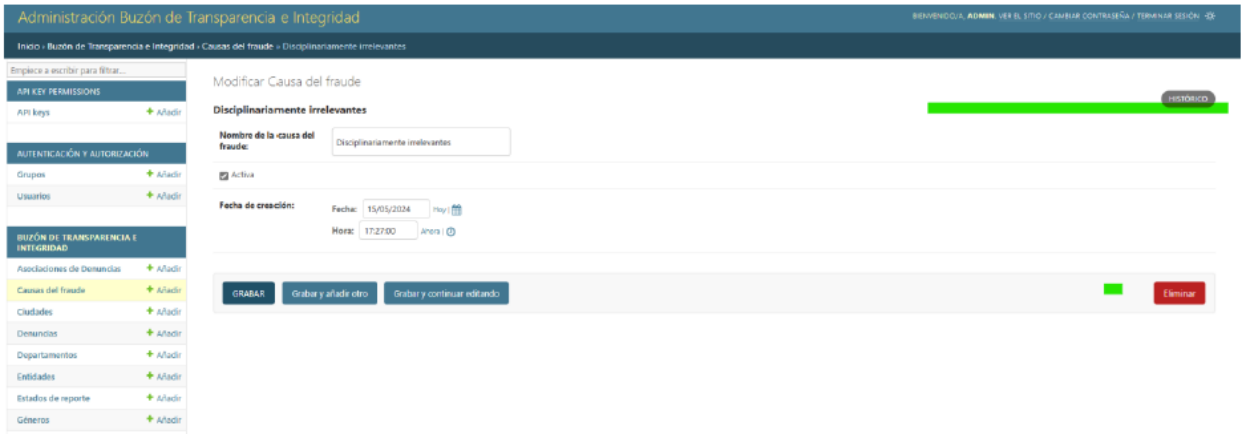


Imagen 3. Modulo de auditoria Buzón de integridad y transparencia

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

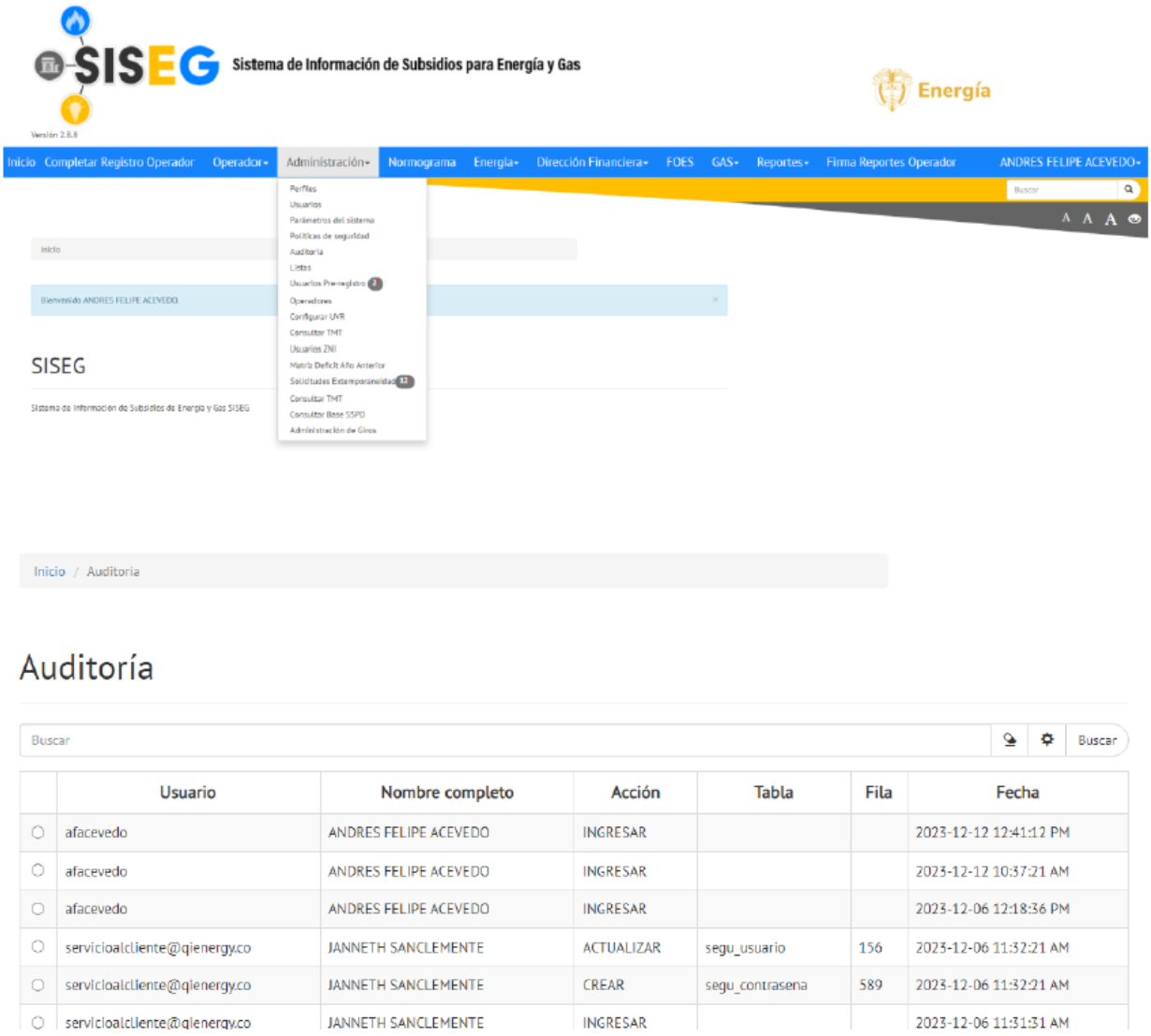


Imagen 5. Módulo de auditoria SISEG.

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

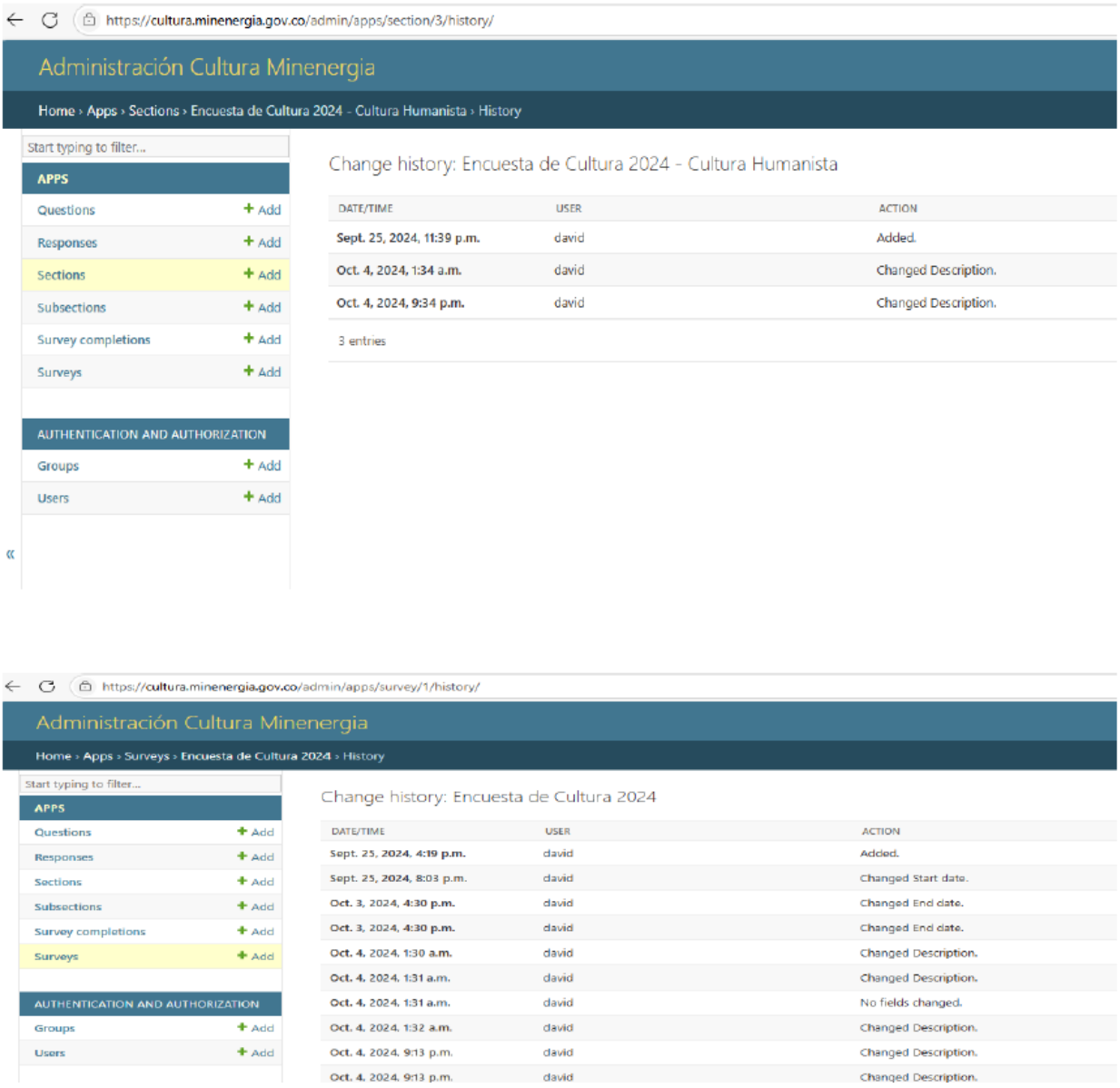


Imagen 6. Modulo de auditoria Encuesta de medición y cultura organizacional

La siguiente tabla resume el estado actual de la implementación, utilizando el inventario como línea base y reflejando el progreso alcanzado en el T4.

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

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 Cuarto trimestre de 2025: Validación de RTO y RPO

El hito principal del T4 en la gestión de este riesgo fue la ejecución de un ejercicio de restauración

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

controlado, el cual representa la primera validación empírica de los objetivos de recuperación (RTO/RPO) del Ministerio en la vigencia 2025.

- **Activo y escenario:** 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 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.

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

Imagen 7 . Evaluación y avance del proceso de backup general de cinta UDP.

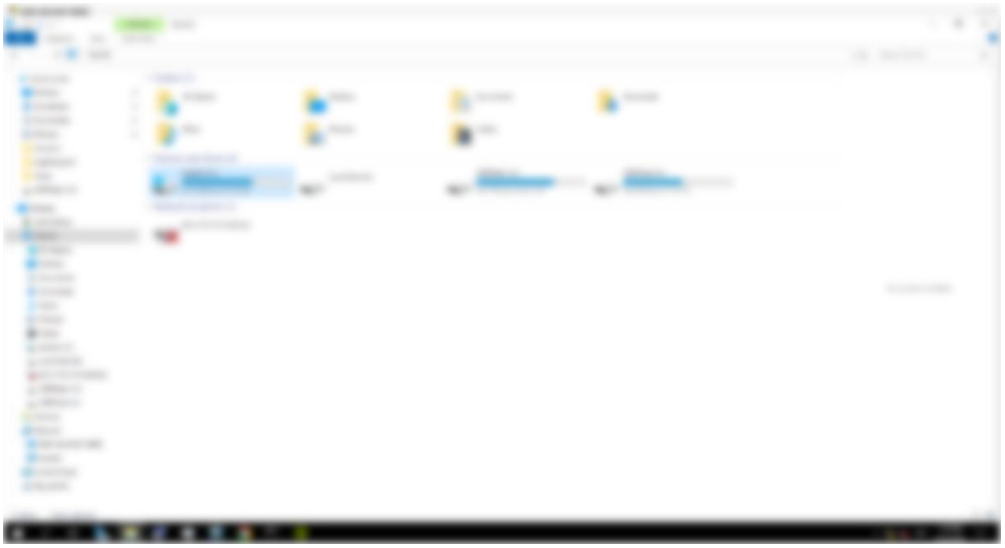


Imagen 8. Repositorio y muestra de espacio de almacenamiento de la infraestructura

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

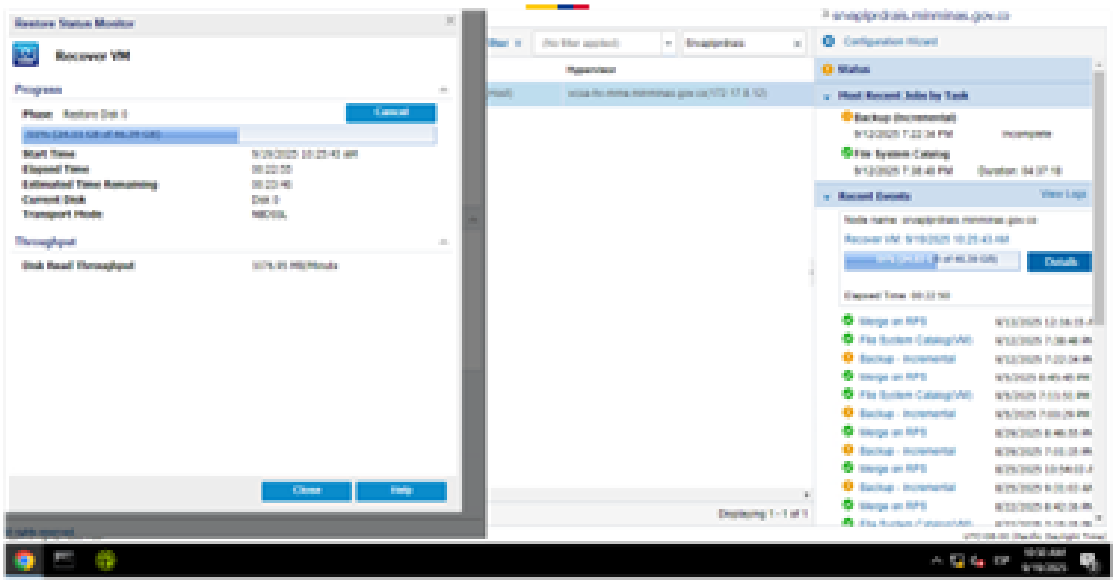


Imagen 9. Proceso de arcservbackup y servidores en proceso

Imagen 10 . 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.

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

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 Cuarto trimestre de 2025: La Institucionalización de la gestión de activos y continuidad

El avance más determinante del T4 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 T3, constituyen la base tecnológica sobre la cual se construirá el DRP actualizado.

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

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

Energía