



Ministerio de
Minas y Energía



Plan de Tratamiento de Riesgos de Seguridad de la Información 2026

Seguimiento Plan de tratamiento de riesgos de seguridad y privacidad de la información

Tercer Trimestre 2026

Elaboró:

Grupo de Tecnologías de la Información y las
Comunicaciones (GTIC)

Leidy Paola Galindo – Coordinadora

Andrés Camilo Molano Mendieta- Seguridad de la
información

Revisó:

Óscar Sánchez Sánchez- Seguridad de la información

Entidad:

Ministerio de Minas y Energía

Bogotá, 30 de Septiembre de 2026

Ministerio de Minas y Energía

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

CONTENIDO

Tabla de contenido

CONTENIDO	3
PROCESO	4
RESPONSABLE DEL PROCESO	4
OBJETIVO.....	4
DESARROLLO DE ACTIVIDADES DE CONTROL DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 2026.....	5
SEGUIMIENTO PLAN DE GESTIÓN	12
CONCLUSIONES Y ACCIONES PRIORITARIAS PARA EL CUARTO TRIMESTRE.....	¡Error!

Marcador no definido.

PROCESO

Gestión tecnológica

RESPONSABLE DEL PROCESO

Grupo de Tecnologías de la Información y las Comunicaciones

Ing. Leidy Paola Galindo

lpgalindo@minenergia.gov.co

Teléfono: (+57) 6012200300 Ext. 2408

OBJETIVO

Documentar el seguimiento y evaluación del Plan de Tratamiento de Riesgos de Seguridad de la Información correspondiente al tercer trimestre de 2026 del Ministerio de Minas y Energía (MINENERGÍA), verificando el estado de los controles, actividades y evidencias asociadas a los riesgos priorizados para la vigencia: R5 – desarrollo seguro e incorporación de IA; R11 – auditoría y monitoreo de sistemas de información; R14 – respaldos y restauración; R21 – activos de información, BIA y BCP; R23 – continuidad y DRP; y el riesgo transversal de cultura de seguridad digital e identidades.

El seguimiento conserva el enfoque por escenarios, servicios y capacidades definido en el Plan 2026 y se sustenta en la evidencia aportada para el periodo. Cuando un soporte contiene datos operativos sensibles, el informe publica únicamente resultados agregados y anonimiza direcciones IP, usuarios, seriales, rutas, credenciales y nombres técnicos con “XXX”. La ausencia de evidencia en el paquete recibido se registra como “pendiente de evidencia”, sin asumir automáticamente que la actividad no fue ejecutada.

Ministerio de Minas y Energía

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

Conmutador: +57 (601) 220 0300

Criterio de publicación y protección de información sensible



Imagen 1. Criterio de anonimización aplicado al seguimiento de riesgos.

Fuente: elaboración propia para publicación del seguimiento.

La valoración del riesgo residual para la vigencia 2026 se sustenta en los resultados del Plan de Tratamiento de Riesgos 2025 y en la metodología institucional definida en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (Versión 6, DAFP), el MSPI de MINTIC, la ISO/IEC 27001:2022 y el NIST Cybersecurity Framework 2.0. El enfoque adoptado en 2026 se basa en servicios, capacidades y escenarios de riesgo, en reconocimiento de la complejidad operativa del Ministerio y la ausencia de una matriz de activos plenamente consolidada.

DESARROLLO DE ACTIVIDADES DE CONTROL DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 2026

Valoración del riesgo residual

La valoración del riesgo residual para la vigencia 2026 se apoya en los resultados del Plan de Tratamiento de Riesgos de Seguridad de la Información 2025 y en la metodología institucional definida en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – Versión 6 del DAFP, el MSPI de MINTIC y la ISO/IEC 27001:2022. Sobre esta base, el grupo de seguridad de la información realizó un análisis integral que combina: i) los riesgos heredados del ciclo anterior (código seguro, auditoría, backups, activos de información y continuidad/DRP) y ii) los riesgos emergentes asociados a la expansión de proyectos de analítica e inteligencia artificial, la gobernanza de datos sectoriales y la cultura de seguridad digital en los funcionarios.

Durante 2025 se consolidaron avances importantes: fortalecimiento del desarrollo seguro mediante DevOps y análisis automático de código (R5), formalización del

Ministerio de Minas y Energía

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

procedimiento de auditoría y despliegue de módulos de logging en sistemas críticos (R11), estabilización operativa de los respaldos con Arcserve UDP y primeras pruebas reales de restauración con medición de RTO/RPO (R14), institucionalización de la gestión de activos de información vía circular 40028 y mesas de trabajo para activos/BIA/BCP (R21), así como la adjudicación del proyecto del Centro de Monitoreo Sectorial (CMS) que proveerá un nuevo CDA y mejores capacidades para el DRP (R23).

No obstante, el análisis evidencia que varios riesgos mantienen un nivel residual relevante: la matriz de activos aún no se encuentra completa ni publicada; el DRP sigue dependiendo de infraestructura en transición; los procesos de backup carecen de un programa formal de pruebas periódicas; y el aumento de soluciones IA y de explotación de datos personales/sensibles introduce nuevos riesgos sobre privacidad, sesgos, uso indebido de la información y exposición reputacional. Adicionalmente, persisten brechas de cultura de seguridad en el manejo de credenciales, contraseñas y MFA, que incrementan la probabilidad de incidentes de compromiso de cuentas. Por ello, para 2026 se mantiene la atención sobre los riesgos R5, R11, R14, R21 y R23, y se incorpora de forma explícita un riesgo transversal de cultura y gestión de identidades digitales, articulado con los proyectos de IA y gobernanza de datos del sector .

Tabla 1. Logros de cada uno de los riesgos del “plan de tratamiento de riesgos 2025”

Riesgo	Conclusión
R5 – Implementación de código seguro y DevOps	Se consolidó la metodología de desarrollo seguro en el “Manual – Metodología y Arquitectura de Referencia para el Desarrollo de Sistemas de Información”, integrando estándares como OWASP y PCI DSS. Se pusieron en marcha pipelines CI/CD en GitLab con validaciones automáticas de estilo de código, dependencias y QA, se habilitó un repositorio privado de imágenes Docker en Nexus y se implementó un clúster de Kubernetes con SonarQube para análisis estático. Al cierre del T3 se había mitigado la mayoría de vulnerabilidades altas y medias identificadas, fortaleciendo el SDLC y la trazabilidad de versiones.



**Ministerio de
Minas y Energía**



R11 – Auditoría y monitoreo de sistemas de información	Se levantó un inventario detallado de SI con y sin capacidades de auditoría, se formalizó el “Procedimiento estándar para la implementación de módulos de auditoría” y se habilitaron o reforzaron módulos de logs en sistemas priorizados (SIMINERO, SISEG, GLPI, Buzón de Integridad y Transparencia, Ventanilla Única de Trámites), diferenciando aquellos que no requieren auditoría transaccional (como GEOVISOR). Esto permitió pasar de acciones aisladas a una hoja de ruta clara de monitoreo y trazabilidad.
---	--

Riesgo	Conclusión
R14 – Gestión de backups y restauración	Se avanzó en la consolidación del appliance Arcserve UDP, con más de 160 servidores respaldados a disco y un número importante en proceso de migración; se ejecutó una depuración progresiva de puntos de restauración, liberando capacidad de almacenamiento y reactivando backups críticos de correo y bases de datos.
R21 – Falencias en la clasificación de activos de información, BIA y BCP	Se diseñó e implementó el instrumento único de gestión de activos de información, integrando catálogos de licenciamiento, SI e infraestructura y ajustándolo a los nuevos lineamientos del MSPI 2025. Se expidió la Circular 40028 de 2025 desde la Secretaría General, asignando enlaces por dependencia y formalizando la obligación de diligenciar la matriz de activos, así como de actualizar los BIA y BCP, lo que elevó el ejercicio de un esfuerzo del Grupo TIC a un compromiso institucional.

Ministerio de Minas y Energía

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





**Ministerio de
Minas y Energía**



R23 – Continuidad del negocio y DRP (CDA/CMS)	Se avanzó en la evaluación de alternativas de colocación y herramientas de respaldo con almacenamiento inmutable y replicación entre centros de datos. En el T3 se legalizó y adjudicó el proyecto del Centro de Monitoreo Sectorial (CMS), que incluye la implementación de un nuevo CDA, capacidades NOC/SOC y una arquitectura de seguridad en profundidad. Este proyecto se convierte en el habilitador principal para actualizar y robustecer el DRP institucional durante 2026.
--	---

Fuente: Elaboración Propia

Tras este balance, se concluye que los controles ejecutados en 2025 han reducido de manera significativa el riesgo inherente en los ámbitos de desarrollo, auditoría, respaldos, clasificación de activos y continuidad; sin embargo, subsiste un riesgo residual que requiere continuidad en 2026, especialmente en lo relacionado con: i) completar y publicar la matriz de activos y los BIA/BCP, ii) poner en operación el nuevo CDA/CMS con un DRP probado, iii) convertir las pruebas de restauración en un programa periódico,) cubrir en el análisis y tratamiento de riesgos los nuevos escenarios ligados a IA, analítica y cultura de seguridad de los usuarios.

Dicho lo anterior se define los siguientes riesgos que contemplan un riesgo residual y nuevos riesgos a trabajar en la vigencia 2026:

Tabla 2. Tabla de riesgos para vigencia 2026

Riesgo	Nombre del riesgo	Actividades necesarias
---------------	--------------------------	-------------------------------

Ministerio de Minas y Energía

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





**Ministerio de
Minas y Energía**



N° R5 Desarrollo seguro	Fallas de seguridad en el ciclo de desarrollo, implementación y uso de IA en software, con riesgo de exposición de información confidencial y datos personales sensibles	1) Actualizar la metodología de desarrollo seguro incorporando soluciones de IA y tratamiento de datos personales sensibles. 2) Estructuración de los lineamientos y políticas de uso, desarrollo e implementación de IA dentro de la entidad 3) Definir, documentar e implementar un procedimiento de revisión de código seguro (code review) basado en buenas prácticas (OWASP, inyección, gestión de errores, autenticación, manejo de datos personales), usando checklists y revisiones entre pares, sin depender de herramientas pagas. 4) Realizar revisiones periódicas de seguridad en el código y la configuración de las aplicaciones críticas.
N° R14 Backups	Gestión integral de respaldos y pruebas de restauración	1) Elaborar y aprobar el procedimiento formal de respaldo y restauración de backups (frecuencia,

Ministerio de Minas y Energía

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





**Ministerio de
Minas y Energía**



		responsables, tipos de copia, priorización de servicios). 2) Definir y ejecutar un programa anual de pruebas de restauración sobre sistemas críticos coordinado con el DRP. 3) Alinear la configuración de la nueva herramienta de respaldo (cuando se despliegue desde el CMS/CDA) con los RTO/RPO definidos en BIA/BCP, en caso de no poder adquirirla se procede a hacer las pruebas con la herramienta actual ArcServ
Nº R 21 Activos/BIA/BCP	Clasificación de activos de información, BIA y BCP actualizados	1) Culminar el diligenciamiento completo de la matriz de activos de información con todos los enlaces designados y consolidar la información a más tardar en mayo. 2) Actualizar los BIA y BCP a partir de la matriz, priorizando procesos misionales y sistemas críticos del sector. 3) Publicar y socializar la versión oficial de la matriz y los planes de continuidad a partir de junio, incluyendo su alineación con el MSPI y el Modelo Integrado de Planeación y Gestión (MIPG).

Ministerio de Minas y Energía

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

Conmutador: +57 (601) 220 0300





**Ministerio de
Minas y Energía**



Nº R23 Continuidad/DRP	Gestión de continuidad y DRP soportado en el nuevo CDA/CMS	1) Actualizar el DRP institucional incorporando la arquitectura del Centro de Monitoreo Sectorial y el nuevo CDA, incluyendo escenarios de ciberataque, fallas de infraestructura y pérdida de datos.
		2) Coordinar al menos un simulacro de recuperación integral que combine restauración de respaldos, conmutación al CDA y validación de operación de servicios críticos. 3) Ajustar el DRP con base en las lecciones aprendidas de los simulacros y en la información proveniente de la matriz de activos, BIA y BCP.

Ministerio de Minas y Energía

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





Ministerio de Minas y Energía



Cultura identidades	e Cultura de seguridad digital y gestión de identidades (contraseñas y MFA)	1) Diseñar e implementar un programa de sensibilización y capacitación con enfoque proactivo y diversas temáticas relacionadas a la seguridad y privacidad de la información. 2) Revisar y ajustar las políticas de contraseñas y de uso de MFA para alinearlas con el MSPI y la ISO/IEC 27001, fomentando su adopción progresiva en los sistemas priorizados. 3) Realizar ataques simulados o señuelo hacia los funcionarios y contratistas de la entidad con el fin de establecer métricas trimestrales que establezcan y relacionen brechas de seguridad digital.
--------------------------------	---	--

SEGUIMIENTO PLAN DE GESTIÓN

La consolidación de evidencias del tercer trimestre permite diferenciar cuatro estados: controles con evidencia operativa suficiente; controles con avance alto pero pendientes de validación; controles con hallazgos que requieren corrección; y actividades programadas para las que no se aportó evidencia concluyente. La tabla siguiente resume la situación antes de desarrollar cada riesgo en detalle.

Tabla 3. Resumen ejecutivo del seguimiento al Plan de Tratamiento de Riesgos — T3 2026

Ministerio de Minas y Energía

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





Ministerio de Minas y Energía

Riesgo	Estado T3 2026	Evidencia principal
R5	Parcial avanzado	Informe T3 de desarrollo seguro: GitLab/MR, Jenkins, Trivy, Registry/Nexus, Kubernetes y VUT.
R11	Parcial avanzado	Módulos/logs en VUT y X-Road; antecedentes en otros SI.
R14	Avance alto con hallazgo	42 jobs, 105 objetos, 49 sesiones exitosas; pruebas de restore y backup granular.
R21	Avance alto	87 % de BIA/BCP; matriz e informe institucional en construcción.
R23	Parcial	Recuperación puntual de VM y alta disponibilidad de componentes.
Cultura e identidades	Avance alto parcial	Tres capacitaciones con evaluación; depuración de accesos/VPN.

5.1 Riesgo R5: Fallas de seguridad en el ciclo de desarrollo, implementación y uso de IA en software

El riesgo R5 busca reducir vulnerabilidades originadas en el desarrollo, integración y despliegue de software y, cuando aplique, en el uso de inteligencia artificial y tratamiento de datos personales o sensibles. La principal evidencia del tercer trimestre es el informe de seguimiento a lineamientos y prácticas de desarrollo, que toma la Ventanilla Única de Trámites (VUT) como caso de aplicación y documenta arquitectura, gestión de requerimientos, seguridad, pruebas, prácticas DevOps/DevSecOps y oportunidades de mejora.

El flujo técnico identificado incorpora control de versiones en GitLab, revisión de cambios mediante Merge Request, automatización con Jenkins, análisis de vulnerabilidades con Trivy, almacenamiento/versionamiento de artefactos en Registry/Nexus y despliegue en Kubernetes para ambientes de QA y producción. Este flujo fortalece la trazabilidad del código y permite integrar controles de seguridad antes de la liberación. El propio informe aclara que la presencia de estas herramientas no permite asumir cobertura institucional uniforme: se debe validar su aplicación por sistema, tecnología y pipeline.

Ministerio de Minas y Energía

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



Flujo DevOps / DevSecOps evidenciado en el seguimiento



Trazabilidad requerida: requerimiento → cambio de código → pipeline → artefacto → versión desplegada

Imagen 2. Flujo DevOps/DevSecOps evidenciado en el seguimiento de desarrollo seguro.

Fuente: elaboración propia con base en el informe de seguimiento T3 de desarrollo de software.

Para la VUT se documentan controles de autorización en backend, roles y permisos, protección de documentos internos, restricción de información sensible en logs, validación de cargas de archivos y trazabilidad en integraciones. También se identifican pruebas unitarias, funcionales, de integración, seguridad, carga/estrés y regresión. La evidencia de escaneo incluida en el informe muestra cero hallazgos críticos y cero altos para el caso revisado, pero este resultado no debe extrapolarse a otros sistemas.

En inteligencia artificial, el informe T3 es explícito en señalar que, dentro del alcance documental revisado, no existe evidencia suficiente para afirmar que los sistemas evaluados incorporaron componentes de IA durante el periodo. Esta limitación es relevante: el control debe activarse cuando exista un desarrollo real y deberá documentar finalidad, modelo o servicio utilizado, datos procesados, autenticación/autorización, secretos, registros, tratamiento de información sensible y dependencias externas. Por lo tanto, el frente de IA se mantiene abierto sin inventar una implementación no demostrada por la evidencia.

Tabla 4. Seguimiento de actividades del riesgo R5

Actividad 2026	Estado T3	Evidencia	Acción pendiente
Actualizar metodología de desarrollo seguro	Avance alto	Prácticas de arquitectura, backlog, seguridad, pruebas y DevSecOps documentadas.	Formalizar cobertura institucional y evidencias mínimas por proyecto.



**Ministerio de
Minas y Energía**

Actividad 2026	Estado T3	Evidencia	Acción pendiente
Lineamientos de uso/desarrollo de IA	Pendiente de evidencia específica	El informe T3 no atribuye IA a los sistemas evaluados.	Aplicar y documentar controles cuando exista un caso verificable.
Code review y trazabilidad	Parcial avanzado	Merge Request y control de versiones identificados.	Relacionar HU/requerimiento con commit, MR, pipeline y despliegue.
Revisión periódica de seguridad	En ejecución	Análisis de vulnerabilidades y controles de WAF/perímetro.	Consolidar cronograma, resultados, remediación y retest.

5.2 Riesgo R11: Auditoría y monitoreo de sistemas de información

El riesgo R11 se orienta a garantizar que las operaciones relevantes sobre los sistemas de información cuenten con trazabilidad suficiente para identificar quién realizó una acción, cuándo se ejecutó, sobre qué objeto y con qué resultado. La evidencia aportada incluye un informe de mecanismos de auditoría y logs que documenta módulos existentes y frentes aún pendientes.

La Ventanilla Única de Trámites cuenta con un módulo de auditoría que registra operaciones de creación, modificación y eliminación y permite consultar usuario, fecha, módulo, funcionalidad e información asociada al cambio. El informe describe almacenamiento del registro antes y después de una modificación, así como opciones de comparación. En la plataforma de interoperabilidad X-Road se evidencia el archivo audit.log del Security Server, con eventos que incluyen fecha/hora, identificador de correlación, tipo de evento, usuario, origen, mecanismo de autenticación y recurso consultado. El correlation-id fortalece el seguimiento de una operación a través de eventos relacionados.

Para el Carnet Virtual Institucional y Mina del Conocimiento, la propia evidencia indica que aún no se cuenta con soporte técnico suficiente para documentar completamente los mecanismos de auditoría y generación de logs. En consecuencia, estos componentes permanecen como pendientes de validación y no deben declararse cerrados.

Ministerio de Minas y Energía

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



Tabla 5. Estado de mecanismos de auditoría revisados

Sistema / frente	Evidencia	Estado de riesgo	Pendiente
VUT	Módulo de auditoría con trazabilidad de CRUD y comparación.	Control evidenciado	Validar cobertura de tablas/modelos y retención.
X-Road	audit.log con eventos de autenticación y correlación.	Control evidenciado	Formalizar revisión periódica y alertamiento.
Otros SI con módulos históricos	Inventario y capturas de módulos disponibles.	En seguimiento	Actualizar inventario y justificar excepciones.
Carnet Virtual	Evidencia técnica insuficiente.	Pendiente	Validar accesos, eventos y retención de logs.
Mina del Conocimiento	Evidencia técnica insuficiente.	Pendiente	Validar trazabilidad documental y eventos de seguridad.

5.3 Riesgo R14: Gestión integral de respaldos y pruebas de restauración

R14 presenta uno de los mayores avances técnicos del trimestre y, al mismo tiempo, un hallazgo que demuestra por qué el plan exige pruebas de restauración. El informe estratégico de respaldos documenta una plataforma con 42 jobs activos y 105 objetos protegidos, organizados por criticidad y frecuencia. La arquitectura combina snapshots locales para recuperación rápida y un repositorio deduplicado para retención de mayor duración. En un corte de 24 horas se registran 49 ejecuciones exitosas sobre 28 jobs distintos, consistentes con las cadencias observadas.

Arquitectura resumida de protección y retención evidenciada



El esquema combina recuperación rápida y retención de mayor duración; las cargas residuales requieren cierre de migración.

Imagen 3. Arquitectura resumida de protección de datos utilizada como evidencia de R14.

Fuente: elaboración propia con base en el informe estratégico de backup, agosto de 2026.

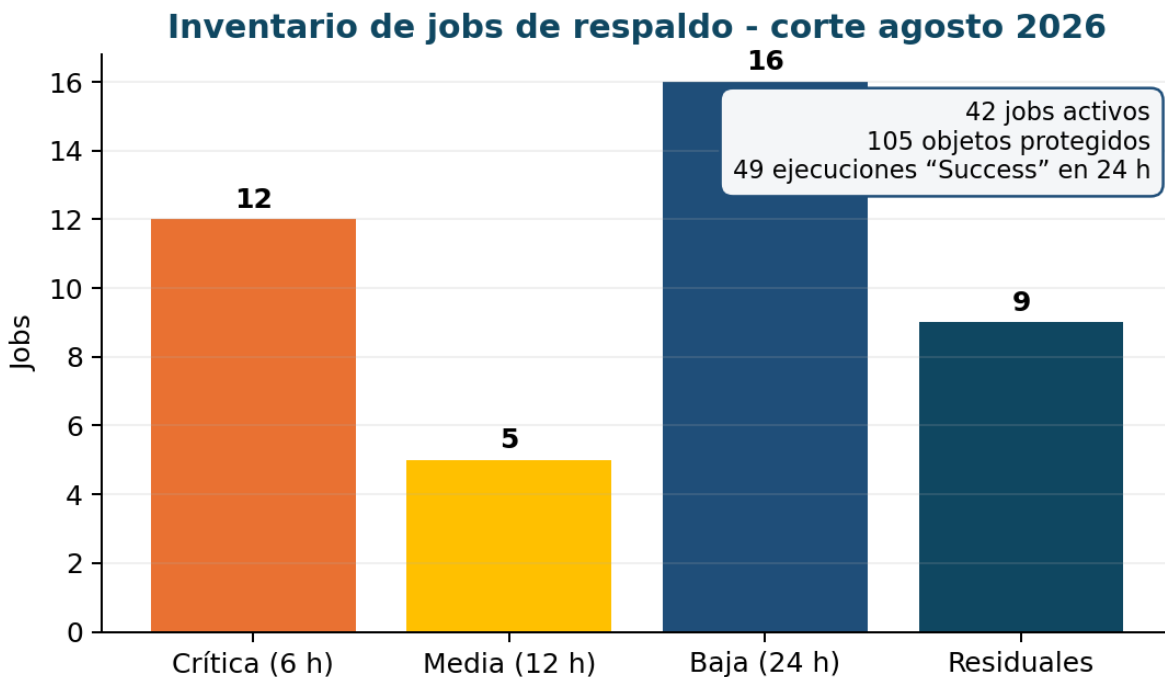


Imagen 4. Cobertura de jobs y ejecuciones de respaldo documentadas.

Fuente: elaboración propia con base en el informe estratégico de backup.

Las pruebas específicas aportadas incluyen un backup granular de aproximadamente 9,8 TB de información de correo, cuya ejecución finalizó con integridad reportada como consistente, aunque se registró una advertencia relacionada con la indisponibilidad del **Ministerio de Minas y Energía**

agente invitado para indexación. También se aportaron ejecuciones de backup granular sobre volúmenes de aproximadamente 1,08 TB y 2,2 TB, concluidas como consistentes por los informes técnicos.

En restauración se observan dos resultados diferentes. Una recuperación controlada de una máquina virtual crítica de aproximadamente 300 GB registró un intervalo de 3 minutos y 2 segundos entre inicio y finalización y reportó integridad consistente. En cambio, una restauración granular de 88,62 MB finalizó técnicamente en aproximadamente 3 minutos y 25 segundos, pero el informe concluye que el bloque no es consistente y que no se restauró la totalidad de la información requerida, posiblemente por problemas de acceso al servidor de archivos. Este resultado mantiene el riesgo abierto hasta que exista causa raíz, corrección y nueva prueba satisfactoria.

Resultados de pruebas de respaldo y restauración aportadas - T3 2026

VM crítica (300 GB)	Éxito
Restauración granular (88,62 MB)	Parcial / Inconsistente
Backup granular (correos 9,8 TB)	Éxito con advertencia
Backup granular (File Server)	Éxito*
Backup granular (File User)	Éxito*

* Los informes de backup granular contienen inconsistencias de fecha/duración que deben corregirse documentalmente.

Imagen 5. Resultado de pruebas de respaldo y restauración aportadas para R14.

Fuente: elaboración propia con base en los informes técnicos de agosto y septiembre de 2026.

Tabla 6. Seguimiento de actividades del riesgo R14

Actividad 2026	Estado T3	Evidencia	Acción pendiente
Operación de plataforma de respaldo	Avance alto	42 jobs / 105 objetos; 49 sesiones “Success” en el corte analizado.	Completar migración/cobertura residual y

Ministerio de Minas y Energía

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

Actividad 2026	Estado T3	Evidencia	Acción pendiente
			mantener monitoreo.
Pruebas periódicas de backup	Ejecutadas	Pruebas granulares sobre distintos volúmenes.	Corregir inconsistencias documentales y normalizar plantillas.
Pruebas de restauración	Ejecutadas con hallazgo	VM crítica satisfactoria; restauración granular incompleta.	Causa raíz, nueva prueba y evidencia de recuperación total.
Alineación RTO/RPO con BIA/BCP	Parcial	BIA/BCP en consolidación.	Mapear jobs, criticidad y tiempos contra RTO/RPO aprobados.

5.4 Riesgo R21: Clasificación de activos de información, BIA y BCP actualizados

El tercer trimestre muestra un avance sustancial en BIA y BCP. El informe de avance del 21 de septiembre reporta 87 % para ambos instrumentos. Por tipo de proceso, los estratégicos y de evaluación y control se encuentran en 100 %, los misionales en 80 % y los transversales en 85,7 %. Se identifican entregables pendientes asociados a un proceso misional y a dos componentes de procesos transversales.

La guía metodológica del BIA se encuentra en revisión y actualización y la matriz maestra se está consolidando y depurando. Esta matriz incorpora servicios/actividades críticas, impactos, recursos, dependencias, sistemas y tiempos MTPD, RTO, RPO y WRT. También se encuentra en elaboración el Informe Institucional BIA, que debe priorizar servicios según impacto y suministrar insumos para BCP, DRP y respaldo.



Ministerio de Minas y Energía

Avance de recepción BIA/BCP - septiembre 2026

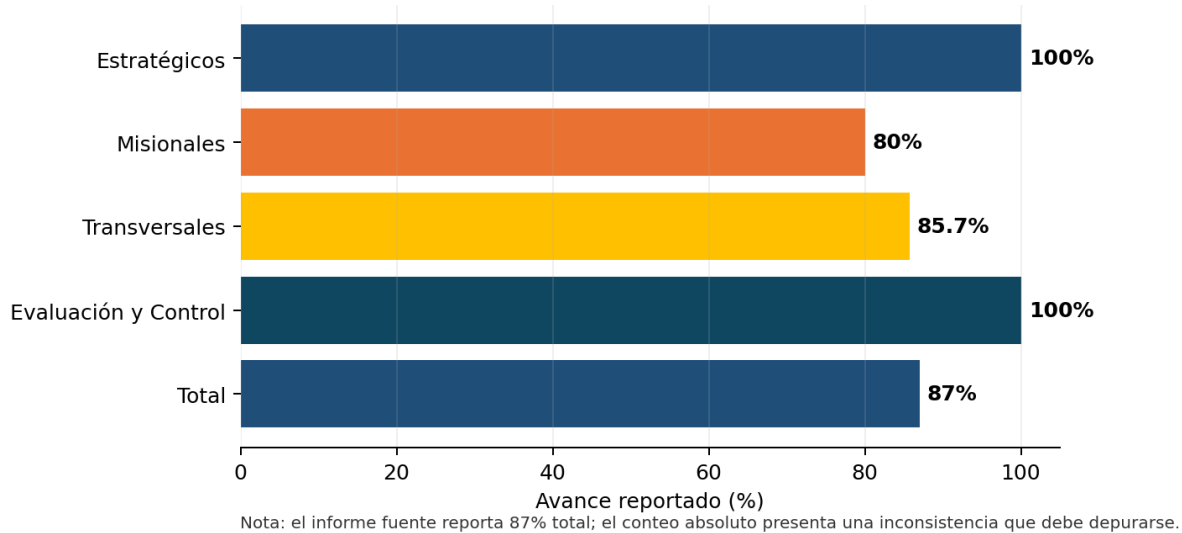


Imagen 6. Avance de BIA/BCP utilizado para el seguimiento de R21.

Fuente: elaboración propia con base en el informe de avance de septiembre de 2026.

La matriz de activos, se encuentra finalizada, dicho artefacto se compone finalmente de 1511 activos de información dentro de la entidad, con la totalidad de los procesos diligenciados, es importante destacar que el siguiente paso es la aceptación de dichos activos por cada uno de los procesos mediante actas de aceptación a cada uno de los líderes del ministerio. A partir, del proceso de gestión de activos de información se procede a la identificación de infraestructura crítica cibernética y la generación de riesgos de seguridad de la información por cada eje en la estructura organizacional del ministerio.

Tabla 7. Seguimiento de actividades del riesgo R21

Actividad 2026	Estado T3	Resultado	Pendiente
Culminar matriz de activos	Finalizado	Se mantiene avance alto; inventario tecnológico actualizado.	Publicación
Actualizar BIA	87 %	Recepción y consolidación institucional en curso.	Cerrar pendientes y corregir conteo.
Actualizar BCP	87 %	Planes recibidos para la mayoría de procesos.	Cerrar pendientes y

Ministerio de Minas y Energía

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



Actividad 2026	Estado T3	Resultado	Pendiente
			validar coherencia con BIA.
Publicar/socializar instrumentos	Parcial	Guía en revisión; informe institucional en elaboración.	Aprobación formal, socialización e integración con SGSI.

5.5 Riesgo R23: Gestión de continuidad y DRP soportado en el nuevo CDA/CMS

El Plan de Tratamiento programó para el segundo semestre la actualización del DRP incorporando la arquitectura de continuidad, la ejecución de un simulacro integral y el ajuste del plan con base en lecciones aprendidas. La evidencia del tercer trimestre aporta elementos habilitadores, especialmente pruebas de recuperación, disponibilidad de componentes y avance BIA/BCP, pero no contiene un documento de DRP actualizado ni un informe de conmutación al Centro de Datos Alterno.

La prueba de recuperación de una VM crítica demuestra que la plataforma de respaldo puede montar y recuperar una carga dentro de un intervalo corto en el escenario controlado documentado. Los reportes mensuales muestran alta disponibilidad del firewall y del WAF, con la observación del periodo sin monitoreo del WAF en agosto. Estos resultados son positivos para la resiliencia, pero corresponden a controles parciales. Un simulacro DRP requiere validar dependencias, red, autenticación, datos, aplicaciones, operación, comunicaciones, responsables, RTO/RPO y retorno a la normalidad.

Por tanto, el riesgo R23 se mantiene en estado parcial. Para cierre de vigencia debe existir evidencia de un DRP actualizado y aprobado, definición del alcance del CDA/CMS, selección de servicios críticos con base en BIA, procedimiento de activación, ejecución controlada de conmutación/recuperación, registro de tiempos reales y plan de mejora posterior.

Tabla 8. Seguimiento de actividades del riesgo R23



Ministerio de Minas y Energía

Actividad 2026	Estado T3	Evidencia	Brecha
Actualizar DRP institucional	Pendiente de evidencia	BIA/BCP y capacidades de backup aportan insumos.	No se aportó DRP actualizado/aprobado.
Simulacro integral de recuperación	Parcial	Existe prueba de recuperación puntual de VM.	No se evidencia conmutación al CDA ni validación integral de servicios.
Ajustar DRP con lecciones aprendidas	Pendiente	Se identifican hallazgos de restauración granular.	Requiere simulacro integral e informe de lecciones aprendidas.
Disponibilidad de controles habilitadores	Avance alto	Firewall/WAF y backup operativos.	Integrar métricas con escenarios y RTO/RPO.

5.6 Riesgo transversal: Cultura de seguridad digital y gestión de identidades

La evidencia del tercer trimestre demuestra continuidad del programa de capacitación y sensibilización. Se ejecutaron tres sesiones virtuales en julio, agosto y septiembre con 54, 58 y 83 personas registradas. Las evaluaciones recibieron 34, 22 y 55 respuestas, con puntuaciones medias de 96,1, 90,9 y 79,3. La existencia de instrumentos de evaluación mejora la capacidad de medir apropiación y permite identificar temas que requieren refuerzo.

Ministerio de Minas y Energía

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





Ministerio de Minas y Energía

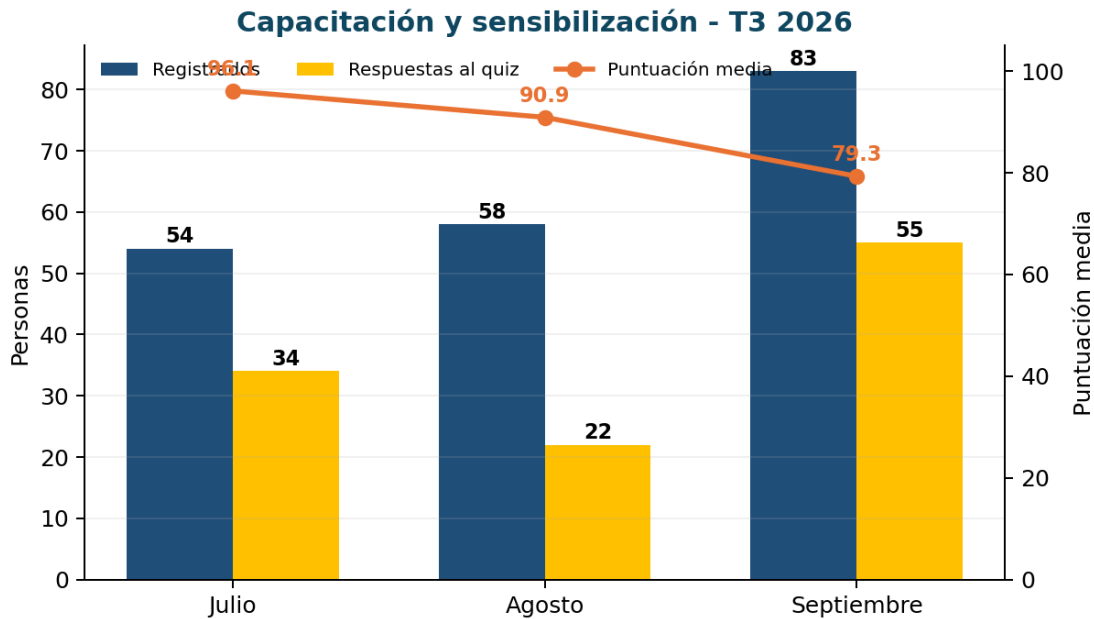


Imagen 7. Resultados de capacitación asociados al riesgo transversal de cultura.

Fuente: elaboración propia con base en el informe de capacitaciones T3 2026.

En gestión de identidades y accesos, el informe de afinamiento registra depuración de usuarios locales y VPN que ya no se utilizan. El reporte VPN SSL del trimestre contiene trazabilidad de conexiones, duración y volumen, pero por razones de publicación no se reproducen usuarios ni patrones individuales. Esta información debe emplearse internamente para identificar cuentas inactivas, accesos anómalos, necesidad de MFA y revisión periódica de privilegios.

No se aportó evidencia de un ataque simulado o señuelo durante T3 ni de la aprobación definitiva de una política institucional de MFA/contraseñas. En consecuencia, el riesgo presenta avance alto en sensibilización y operación, pero mantiene pendientes dos actividades relevantes del plan: medición mediante ejercicio simulado y formalización/seguimiento de controles de autenticación.

Tabla 9. Seguimiento del riesgo transversal de cultura e identidades

Actividad	Estado T3	Evidencia	Pendiente
Programa de sensibilización	Cumplido T3	Tres capacitaciones con material, asistencia y quiz.	Mantener periodicidad y medir tendencia.
Revisión de identidades/accesos	En ejecución	Depuración de usuarios locales y VPN.	Integrar recertificación de accesos y

Ministerio de Minas y Energía

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





Ministerio de Minas y Energía

Actividad	Estado T3	Evidencia	Pendiente
			mínimo privilegio.
Política de contraseñas y MFA	Pendiente evidencia de cierre	Existe necesidad y de antecedentes implementación.	Aportar aprobación, cobertura y excepciones.
Ataques simulados o señuelo	No evidenciado en T3	No se aportó reporte específico.	Ejecutar o documentar reprogramación y métricas.

5.7 Consolidación del avance del Plan de Tratamiento de Riesgos

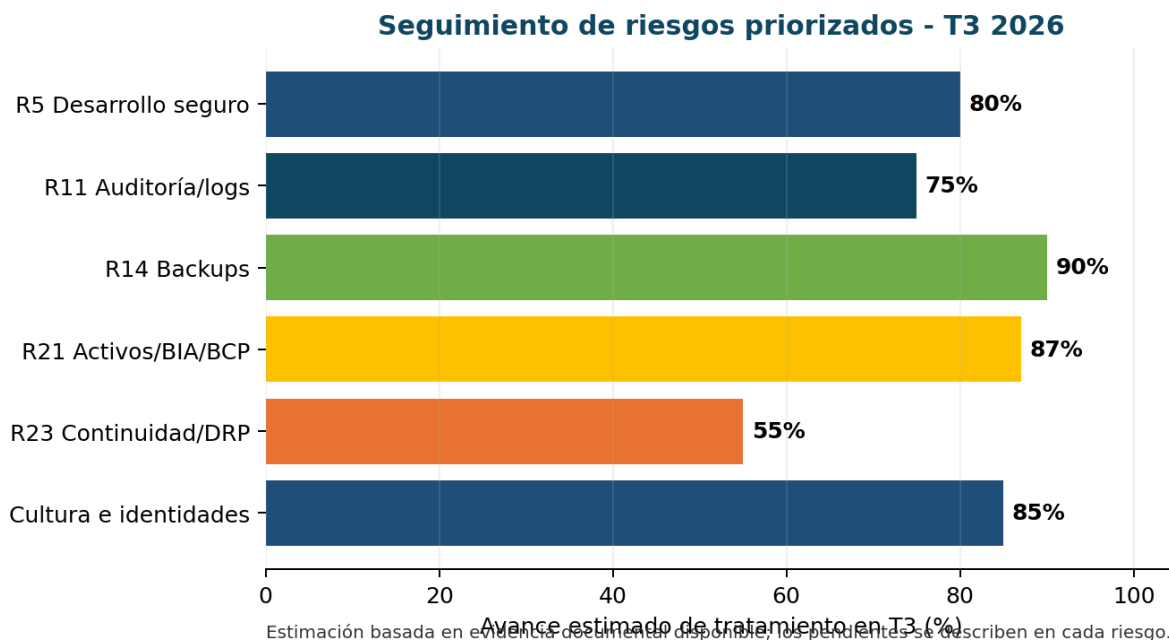


Imagen 8. Avance estimado de los riesgos priorizados en el tercer trimestre.

Fuente: elaboración propia con base en la evidencia suministrada. Estimación de seguimiento, no KPI formal.

Tabla 10. Consolidado de riesgos — T3 2026

Ministerio de Minas y Energía

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





**Ministerio de
Minas y Energía**

Riesgo	Avance estimado T3	Lectura de control
R5 – Desarrollo seguro / IA	80 %	Controles evidenciados; DevSecOps cobertura institucional e IA pendientes.
R11 – Auditoría y logs	75 %	Controles en sistemas priorizados; faltan validaciones de soluciones pendientes.
R14 – Backups y restauración	90 %	Operación robusta y pruebas ejecutadas; hallazgo granular abierto.
R21 – Activos/BIA/BCP	87 %	BIA/BCP avanzados; cierre metodológico e institucional pendiente.
R23 – Continuidad/DRP	55 %	Capacidades habilitadoras disponibles; DRP/simulacro integral no evidenciados.
Cultura e identidades	85 %	Capacitación y depuración de accesos; MFA/simulacro pendientes.

El promedio simple de avance estimado para el trimestre es cercano al 79 %. El valor no representa una recalificación formal de probabilidad e impacto de la matriz institucional; es una lectura de cobertura de las actividades y evidencias del plan. La recalificación del riesgo residual debe realizarse en la matriz oficial mediante la metodología institucional y con participación de los responsables de proceso y de control.

5.8 Calidad, trazabilidad y suficiencia de la evidencia

El tercer trimestre evidencia una mejora en la cantidad y granularidad de soportes, pero también muestra aspectos de gestión documental que deben corregirse antes del cierre anual. Un SGSI auditable requiere que las evidencias sean consistentes en fecha, periodo, responsable, objeto de prueba, resultado, versión de herramienta, unidad de medida y relación con el control evaluado.

Ministerio de Minas y Energía

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

