



Ministerio de
Minas y Energía



Plan de Seguridad y Privacidad de la Información 2026

Seguimiento Plan 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:

Oscar 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	¡Error! Marcador no definido.
RESPONSABLE DEL PROCESO	¡Error! Marcador no definido.
DESCRIPCIÓN DEL INFORME.....	4
PLAN OPERACIONAL DE SEGURIDAD DE LA INFORMACIÓN	5
CONCLUSIONES Y ACCIONES DE CIERRE 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@minenergía.gov.co

Teléfono: (+57) 6012200300 Ext. 2408

OBJETIVO

El presente informe corresponde al seguimiento del tercer trimestre (julio–septiembre de 2026) del Plan de Seguridad y Privacidad de la Información 2026 del Ministerio de Minas y Energía (MINENERGÍA). El documento conserva la estructura utilizada en los seguimientos del primer y segundo trimestre y consolida las evidencias técnicas y de gestión aportadas para el periodo, con énfasis en activos de información, análisis de impacto al negocio y continuidad, tratamiento de riesgos, recursos de seguridad, indicadores, afinamiento de ciberseguridad, gestión de vulnerabilidades, auditoría, comunicaciones, sensibilización y capacitación.

El seguimiento se desarrolla bajo el ciclo de mejora continua del SGSI y mantiene como marco los tres pilares del Plan 2026: consolidación e integración tecnológica; cierre de brechas críticas, particularmente en activos, BIA/BCP, monitoreo y continuidad; y fortalecimiento de la resiliencia y capacidad de recuperación. La valoración se realiza exclusivamente con base en la evidencia suministrada para el corte, por lo que la ausencia de un soporte no se interpreta automáticamente como ausencia de ejecución, sino como una brecha de evidencia que debe ser subsanada para efectos de trazabilidad, auditoría y rendición de cuentas.

Criterio de publicación y protección de información sensible

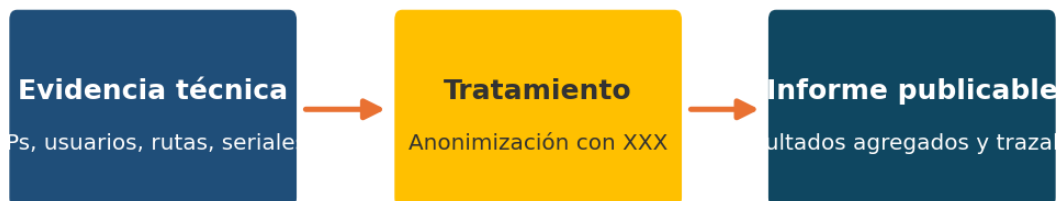


Imagen 1. Criterio aplicado para la publicación de evidencias técnicas.

Fuente: elaboración propia con base en el criterio de publicación utilizado en los seguimientos del SGSI.

Ministerio de Minas y Energía

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

Conmutador: +57 (601) 220 0300

PLAN OPERACIONAL DE SEGURIDAD DE LA INFORMACIÓN

4.1 Gestión de activos de información

La gestión de activos de información continúa siendo un componente estructural del SGSI porque permite relacionar los procesos institucionales con la información que utilizan, los sistemas que la soportan, sus propietarios, dependencias y niveles de criticidad. Al cierre del segundo trimestre se había reportado un avance aproximado del 90 % en la identificación y clasificación, sin que la matriz pudiera declararse cerrada oficialmente. Para el cierre del trimestre el Ministerio de Minas y Energía consolida su matriz de activos de información con todos los procesos en su estructura organizacional, arrojando 1511 activos depurados y sin duplicidad, para mayor información se sugiere validar con el oficial de seguridad de la información de la entidad.

Como evidencia complementaria se recibió un inventario de software generado por la herramienta institucional de gestión de activos con corte al 25 de septiembre de 2026. El reporte consolida software detectado, versiones, fabricante, número de instalaciones y campos de licenciamiento. Este insumo fortalece la visibilidad tecnológica y puede utilizarse para conciliación con los catálogos de activos, licenciamiento y vulnerabilidades; sin embargo, no sustituye la matriz institucional de activos de información, cuyo alcance comprende activos de información, responsables, valoración y relación con procesos.

4.2 Gestión de BIA y BCP

Durante el tercer trimestre se evidencia un avance material en la implementación del Análisis de Impacto al Negocio (BIA) y los Planes de Continuidad del Negocio (BCP). El informe de avance del 21 de septiembre de 2026 reporta un nivel de recepción del 87 % tanto para BIA como para BCP. Por tipo de proceso, los estratégicos y de evaluación y control alcanzan 100 %; los misionales 80 %; y los transversales 85,7 %. Los pendientes identificados se concentran en un proceso misional y en componentes asociados a dos procesos transversales.

La guía metodológica para la implementación del BIA continúa en revisión y validación por parte de la Oficina de Planeación y Gestión Internacional. Paralelamente se adelanta la consolidación y depuración de la matriz institucional, incorporando servicios y actividades críticas, impactos, recursos, dependencias, sistemas asociados y tiempos de recuperación MTPD, RTO, RPO y WRT. Asimismo, se encuentra en elaboración el Informe Institucional de Análisis de Impacto al Negocio, que deberá permitir priorizar procesos y servicios según impactos operativos, legales, financieros, reputacionales y de servicio público.

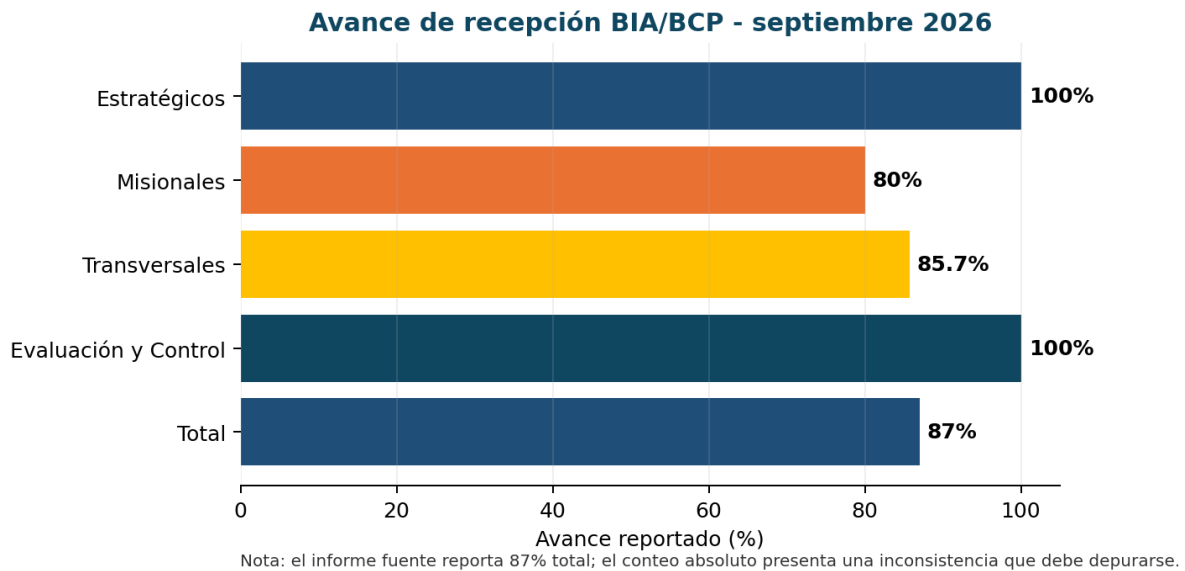


Imagen 2. Avance reportado de BIA y BCP por tipo de proceso.

Fuente: elaboración propia con base en el Informe de Avance BIA/BCP del 21 de septiembre de 2026.

Tabla 2. Estado de instrumentos y actividades BIA/BCP, tercer trimestre 2026

Instrumento	Estado T3 2026	Resultado observado	Pendiente
Guía de implementación BIA	En revisión	Se actualizan criterios de criticidad, impactos, recursos y tiempos de recuperación.	Aprobación, publicación y socialización institucional.
Recepción de BIA	87 %	Avance por procesos: estratégicos 100 %, misionales 80 %, transversales 85,7 %, evaluación y control 100 %.	Cerrar entregables pendientes y validar consistencia.
Recepción de BCP	87 %	Se dispone de planes asociados a la mayoría de procesos evaluados.	Cerrar pendientes y alinear estrategias con BIA validado.
Matriz maestra BIA	En consolidación	Integra servicios, impactos, dependencias y tiempos MTPD/RTO/RPO/WRT.	Depurar diferencias y aprobar versión maestra.
Informe institucional BIA	En elaboración	Se estructura priorización institucional de criticidad.	Emitir informe definitivo y utilizarlo como

			insumo de DRP y respaldos.
--	--	--	----------------------------

4.3 Tratamiento de riesgos de seguridad de la información

El seguimiento del tercer trimestre al Plan de Tratamiento de Riesgos muestra avances relevantes en desarrollo seguro, registros de auditoría, respaldos, BIA/BCP, recuperación y cultura de seguridad. La evidencia también mantiene brechas que impiden considerar varios riesgos como cerrados: no se aporta evidencia de un simulacro integral de DRP con conmutación al Centro de Datos Alterno, una prueba de restauración granular resultó incompleta, persisten entregables BIA/BCP pendientes y no se aporta evidencia suficiente del cierre de los componentes de auditoría de todos los sistemas ni de ejercicios simulados de ingeniería social durante el trimestre.

El detalle de cada riesgo se desarrolla en el documento independiente “Seguimiento del tercer trimestre al Plan de Tratamiento de Riesgos de Seguridad de la Información 2026”. Para efectos del presente Plan de Seguridad y Privacidad, la siguiente tabla resume el resultado ejecutivo del tratamiento.

Tabla 3. Resumen de riesgos priorizados — tercer trimestre 2026

Riesgo / frente	Estado T3	Resultado principal	Pendiente relevante
R5 – Desarrollo seguro / IA	Avance alto	Se evidencian prácticas DevOps/DevSecOps, control de versiones, revisión de cambios, CI/CD, análisis de vulnerabilidades, artefactos y separación QA/Producción.	Demostrar cobertura por sistema y completar evidencia específica de IA cuando aplique.
R11 – Auditoría y logs	Parcial avanzado	Se evidencian mecanismos de auditoría en VUT y X-Road y antecedentes en otros sistemas.	Completar validación técnica de soluciones pendientes y homogeneizar trazabilidad.
R14 – Backups y restauración	Avance alto con hallazgo	La plataforma protege 42 jobs/105 objetos y se ejecutaron pruebas de respaldo y restauración.	Corregir inconsistencia de restauración granular y depurar errores documentales de los informes.
R21 – Activos/BIA/BCP	87 % BIA/BCP	Se consolidan BIA/BCP y matriz maestra.	Cerrar procesos pendientes, aprobar guía y emitir informe institucional.

R23 – Continuidad/DRP	Parcial	Se ejecutó recuperación de una VM crítica y se mantuvo disponibilidad de componentes.	Evidenciar DRP actualizado y simulacro integral con CDA/conmutación.
Cultura e identidades	Avance alto parcial	Tres capacitaciones T3, evaluaciones y depuración de accesos/VPN.	Evidenciar política MFA/contraseñas formalizada y ejercicio simulado o señuelo.

4.4 Gestión de políticas y procedimientos

En el segundo trimestre se había consolidado la formalización de procedimientos de incidentes, vulnerabilidades y cifrado, además del avance de una política de identidades y autenticación. Durante el tercer trimestre las evidencias aportadas se concentran en la aplicación operativa de controles y no en nuevos actos formales de aprobación. Por lo tanto, el seguimiento valora la efectividad práctica de los instrumentos sin afirmar la expedición de documentos que no se encuentran soportados en el paquete documental recibido.

Los informes de respaldo y restauración demuestran aplicación de controles de cifrado, acceso y verificación de integridad; los reportes de seguridad perimetral evidencian actividades de hardening, depuración de usuarios y bloqueo de amenazas; y los informes de desarrollo seguro y auditoría de sistemas muestran aplicación de prácticas de trazabilidad, roles, logs y validaciones técnicas. Esta evidencia demuestra uso de lineamientos del SGSI, aunque debe fortalecerse la relación explícita entre cada actividad y el procedimiento institucional que la gobierna.

Como acción de cierre para el cuarto trimestre, se recomienda consolidar una matriz de vigencia documental del SGSI que relacione documento, código SIG, versión, fecha de aprobación, responsable, evidencia de socialización, controles asociados y fecha de próxima revisión. Esto facilitará demostrar no solo que los documentos existen, sino que se encuentran apropiados y operativos.

Tabla 4. Seguimiento de instrumentos normativos y de operación

Frente	Situación T3	Evidencia	Acción requerida
Gestión de incidentes	En operación	Monitoreo, bloqueo de indicadores de compromiso y coordinación con capacidades especializadas.	Mantener registro de incidentes/eventos y lecciones aprendidas.
Gestión de vulnerabilidades	En operación	Escaneos, controles DevSecOps y lineamientos de remediación/retest.	Consolidar trazabilidad hallazgo–

			responsable–fecha– cierre.
Cifrado y protección de respaldo	Aplicado	Informes de backup/restauración reportan cifrado y control de acceso.	Mantener evidencia de configuración sin exponer secretos.
Identidades y autenticación	Parcial	Depuración de usuarios locales/VPN y seguimiento de accesos remotos.	Aportar evidencia de aprobación y cobertura de MFA/política de contraseñas.
IA y desarrollo seguro	Parcial	Flujo DevSecOps documentado; no se evidencia IA en los sistemas evaluados por el informe T3.	Formalizar lineamientos específicos y aplicar cuando exista un caso verificable.

4.5 Gestión de recursos de seguridad

Durante el tercer trimestre se evidencia utilización sostenida de recursos tecnológicos de seguridad en las capas perimetral, respaldo, recuperación, monitoreo, conectividad remota y gestión de activos. La plataforma de respaldos registra 42 jobs activos y 105 objetos protegidos, con política diferenciada por criticidad y retención en dos niveles. La bitácora analizada para un corte de 24 horas reporta 49 ejecuciones finalizadas correctamente sobre 28 jobs distintos. El esquema combina recuperación rápida sobre la plataforma de virtualización principal y retención extendida en un repositorio deduplicado.

La seguridad perimetral opera en alta disponibilidad. El informe trimestral de afinamiento registra consumos de CPU por debajo del 32 % y memoria entre 51 % y 58 %, dentro de los rangos operativos reportados por el proveedor/administrador. Se realizaron actividades de depuración de políticas, limpieza de usuarios locales y VPN no utilizados y bloqueo de direcciones asociadas a intentos de ataque o indicadores de compromiso. Para publicación se omiten seriales, nombres de equipos y direcciones.

En materia de continuidad, la existencia de pruebas de restauración y de una arquitectura de respaldos más robusta representa un avance frente a los riesgos históricos. No obstante, la evidencia disponible no permite declarar culminada la puesta en operación de un DRP integral con conmutación al CDA/CMS. La recuperación de una máquina virtual o de archivos individuales valida capacidades puntuales, pero no equivale por sí sola a un ejercicio de recuperación de desastre extremo a extremo.

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 y retención evidenciada.

Fuente: elaboración propia con base en el Informe Estratégico de Gestión de Copias de Respaldo, corte 14–15 de agosto de 2026.

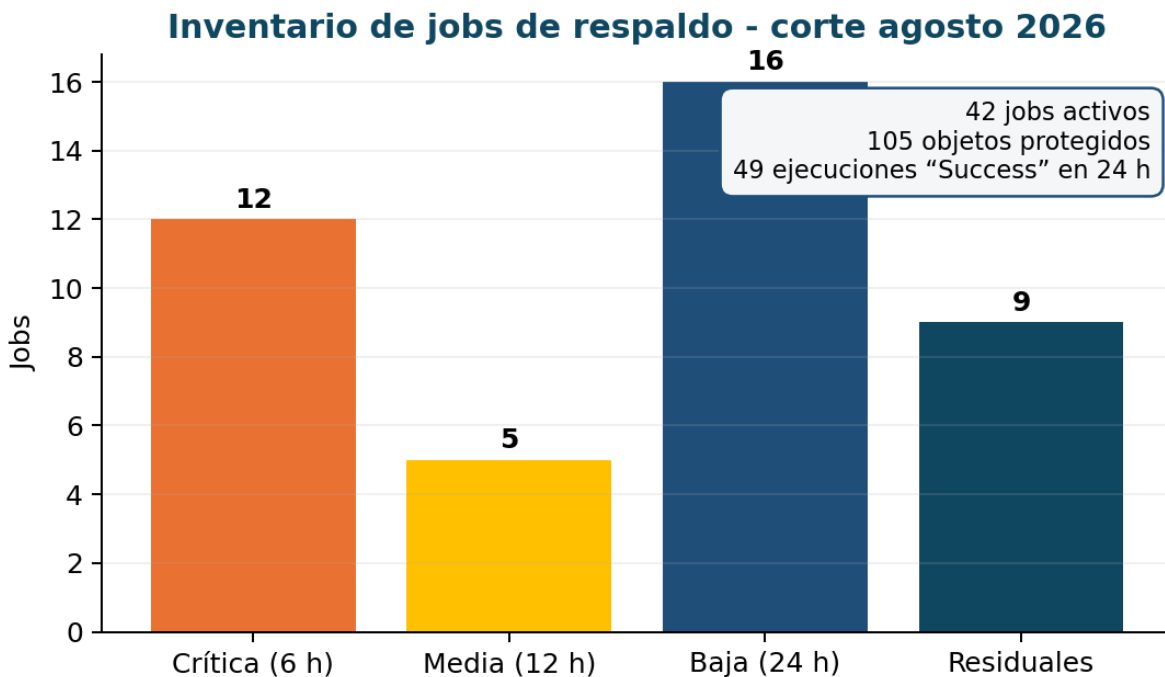


Imagen 4. Distribución de jobs de respaldo y cobertura observada.

Fuente: elaboración propia con base en la consola documentada en agosto de 2026.

Tabla 5. Recursos de seguridad observados en el tercer trimestre

Recurso / capacidad	Estado observado	Resultado	Necesidad de continuidad
Firewall perimetral en HA	Operativo	Disponibilidad reportada del 100 % y recursos	Renovar licenciamiento y

Ministerio de Minas y Energía

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

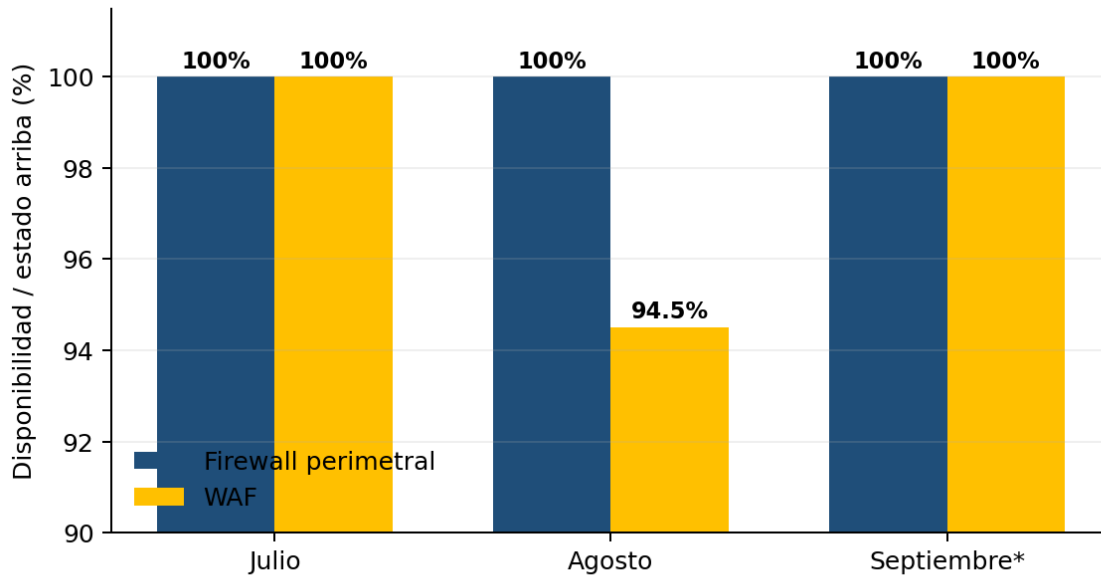
		dentro de rangos normales.	mantener afinamiento/mantenimiento.
WAF	Operativo con observación	Julio y septiembre reportan 100 %; agosto registra 94,5 % “arriba” y 5,5 % “sin monitorizar”.	Explicar y cerrar la ventana sin monitoreo.
Plataforma de respaldo	Operativa	42 jobs activos, 105 objetos y ejecuciones exitosas en el corte analizado.	Cerrar migración de cargas residuales y sostener pruebas.
VPN SSL	Operativa	Existe trazabilidad de conexiones, duración y volumen agregado.	Mantener depuración de cuentas, MFA y alertamiento.
Gestión de activos/software	Operativa	Inventario de software con corte 25/09/2026.	Conciliar con activos de información y licenciamiento.

4.6 Gestión de indicadores de seguridad de la información

El tercer trimestre amplía la base de indicadores disponibles para el SGSI. Además de los indicadores tradicionales de disponibilidad, se cuenta con métricas de respaldo, restauración, avance BIA/BCP, capacitación y accesos remotos. Esto permite avanzar desde una lectura exclusivamente tecnológica hacia una visión que combine disponibilidad, capacidad de recuperación, cultura y madurez documental.

En disponibilidad, el firewall perimetral registra 100 % en los reportes de julio, agosto y septiembre con corte al 28 de septiembre. El WAF registra 100 % en julio, una lectura gráfica de 94,5 % “arriba” y 5,5 % “sin monitorizar” en agosto, y 100 % para el periodo del 1 al 28 de septiembre. Los reportes tabulares del producto muestran 100 % en varias ventanas; por ello, el seguimiento conserva la observación gráfica de agosto y recomienda revisar la causa de la diferencia antes de utilizar un indicador consolidado de SLA.

Disponibilidad observada de componentes de seguridad - T3 2026



* Septiembre con corte al 28/09/2026. En agosto el WAF registró 5,5% del periodo como “sin monitorizar”.

Imagen 5. Disponibilidad observada de componentes de seguridad durante el T3.

Fuente: elaboración propia con base en reportes mensuales de disponibilidad de firewall y WAF.

En respaldos se cuenta con métricas de número de jobs, objetos protegidos, frecuencia y sesiones exitosas. En restauración, una prueba de máquina virtual crítica de 300 GB registra inicio a las 15:06:49 y finalización a las 15:09:51, equivalente a aproximadamente 3 minutos y 2 segundos, con integridad reportada como consistente. En contraste, una prueba granular sobre 88,62 MB finaliza técnicamente pero no recupera la totalidad de la información requerida, por lo que debe tratarse como hallazgo y no como éxito completo.

En BIA/BCP el indicador de recepción es 87 %. En capacitación, se realizaron tres sesiones con 54, 58 y 83 personas registradas respectivamente; los cuestionarios recibieron 34, 22 y 55 respuestas. Las puntuaciones medias fueron 96,1; 90,9 y 79,3. Estas métricas permiten medir alcance y aprendizaje, aunque la caída de la puntuación en septiembre y la menor tasa de respuesta de agosto justifican reforzar mecanismos de participación y evaluación.

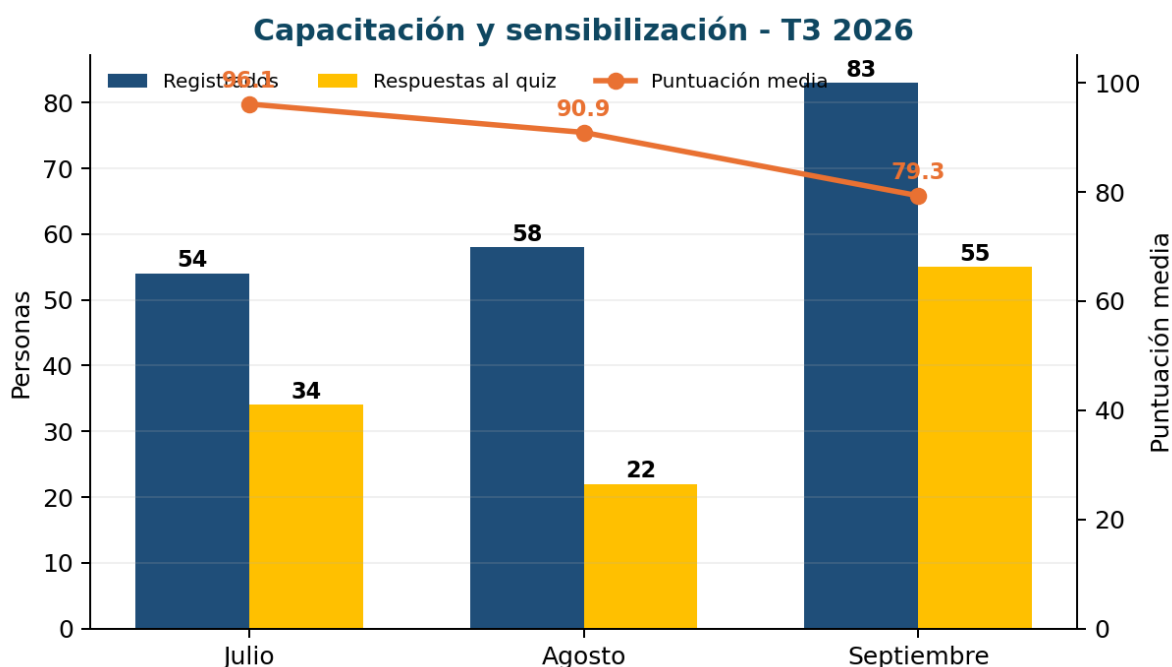


Imagen 6. Participación y resultados de evaluación de las capacitaciones del T3.

Fuente: elaboración propia con base en el Informe de Ejecución y Resultados de Capacitaciones, julio–septiembre de 2026.

Tabla 6. Indicadores ejecutivos para seguimiento del SGSI — T3 2026

Indicador	Resultado observado	Lectura de seguridad
Disponibilidad firewall	100 % en los reportes mensuales aportados.	Estabilidad de la capa perimetral durante las ventanas observadas.
Disponibilidad WAF	100 % julio; 94,5 % arriba / 5,5 % sin monitorizar en agosto; 100 % septiembre*	Revisar la ventana de monitoreo de agosto y documentar causa.
Cobertura de respaldos	42 jobs activos / 105 objetos protegidos.	Cobertura significativa con política por criticidad.
Sesiones de backup exitosas	49 ejecuciones “Success” sobre 28 jobs en 24 h.	Comportamiento consistente con las cadencias documentadas.
Prueba de recuperación VM crítica	Aprox. 3:02 min; integridad consistente.	Evidencia positiva de capacidad de recuperación puntual.
Restauración granular	Finaliza en aprox. 3:25 min, pero no recupera toda la información.	Hallazgo que requiere causa raíz y nueva prueba.
BIA y BCP	87 % de avance reportado.	Avance alto, aún sin cierre institucional.

Capacitación	3 sesiones; 195 registros acumulados; 111 respuestas a quiz.	Cobertura creciente; requiere reforzar evaluación y apropiación.
---------------------	--	--

1. Indicadores de Disponibilidad de Servicios de Seguridad (SLA):

- **Firewall Perimetral** : Se mantuvo un cumplimiento perfecto, registrando una disponibilidad del 100% durante los meses de enero, febrero y marzo.

Gráfico de disponibilidad para el mes pasado

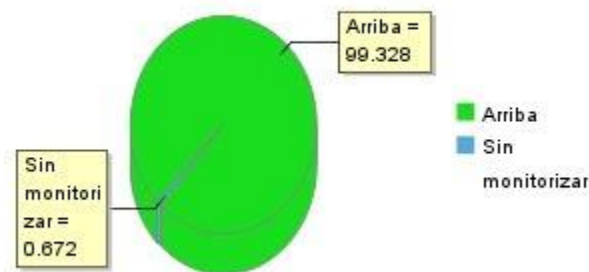


Imagen [7]. Grafico de disponibilidad firewall para el tercer trimestre 2026

Estadísticas de disponibilidad	
Opciones	Tiempo de actividad (%)
Hoy	100.0%
Ayer	100.0%
Ultimos 7 días	100.0%
Ultimos 30 días	100.0%
Los últimos 60 días	100.0%
Los últimos 90 días	100.0%
Esta semana	100.0%
La semana pasada	100.0%
Este mes	100.0%
El mes pasado	100.0%
Este trimestre	100.0%

Imagen [8]. Disponibilidad firewall para el tercer trimestre 2026

- **Web Application Firewall (WAF)**: El servicio operó con una disponibilidad del 99.7% en enero, alcanzó el 100% en abril y presentó una leve disminución al 96.9% en mayo.

Ministerio de Minas y Energía

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

Gráfico de disponibilidad para el mes pasado

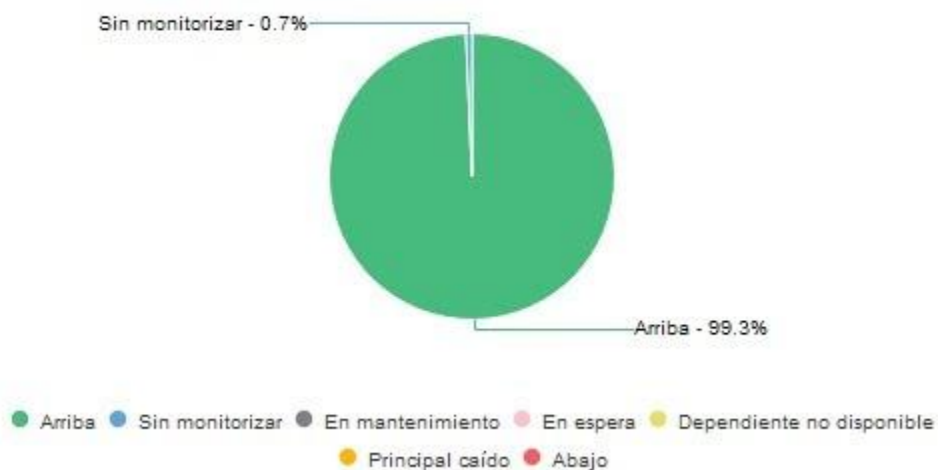


Imagen [9]. Disponibilidad WAF para el mes de julio 2026

Gráfico de disponibilidad para el mes pasado

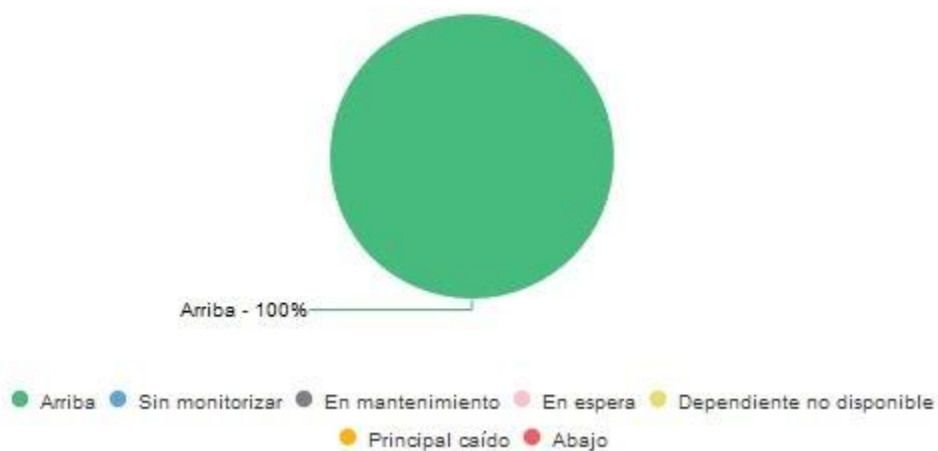


Imagen [10]. Disponibilidad WAF para el mes de agosto 2026

Gráfico de disponibilidad para el mes pasado

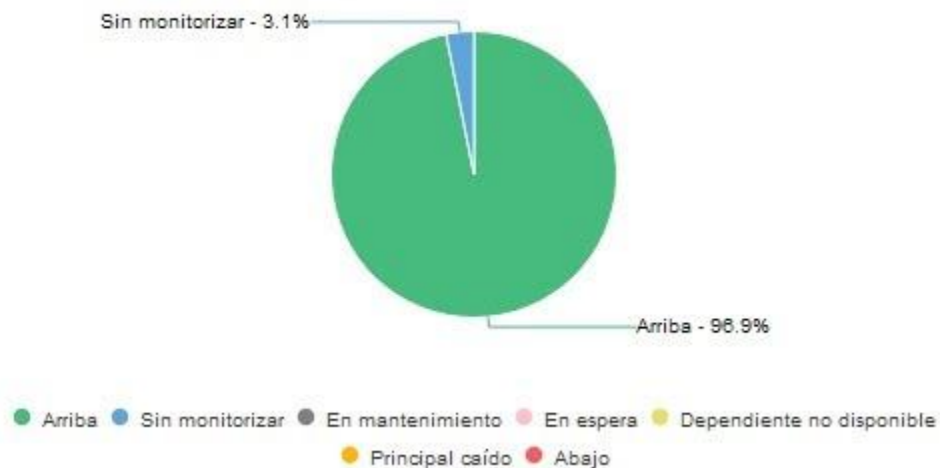


Imagen [11]. Disponibilidad WAF para el mes de septiembre 2026

- **Enlaces de Conectividad (Media Commerce):** La disponibilidad promedio general de los enlaces de datos e internet se mantuvo en el 99.72%, presentando caídas muy puntuales y aisladas en sedes específicas (ej. Item 10 en enero al 0% en un día puntual, e Item 3 en marzo al 0% en días específicos).

2. Indicadores de Protección de Endpoints :

- **Cobertura de licenciamiento:** De un total de XXXX licencias adquiridas, se cerró el mes de septiembre con XXXX licencias en uso. Este indicador subraya la necesidad de acelerar el despliegue del agente en los equipos restantes.

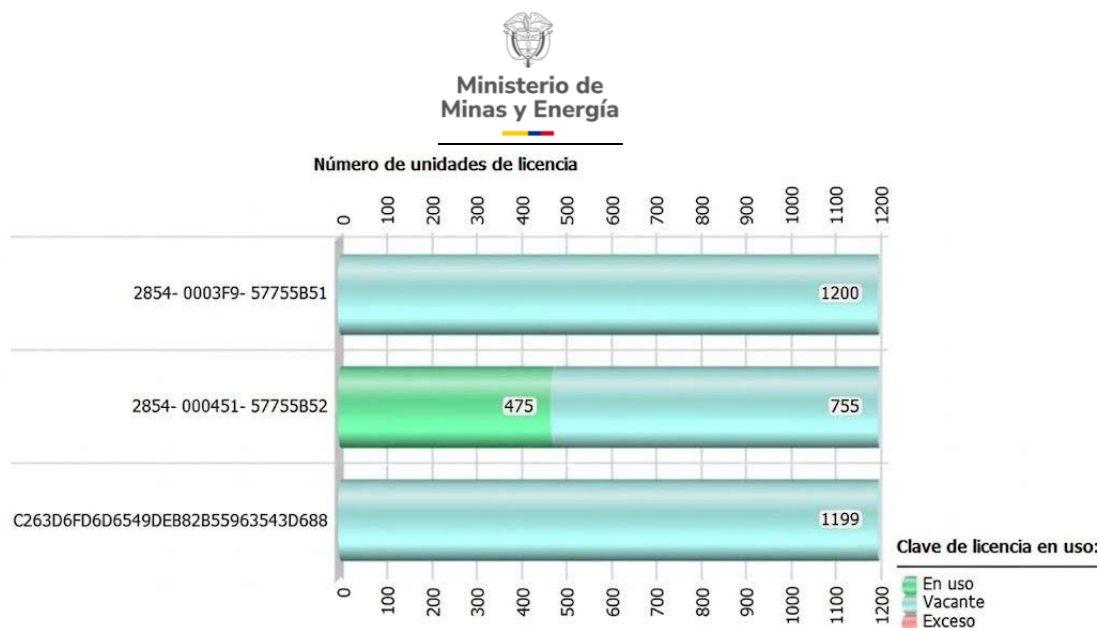


Imagen [12]. Licenciamiento de endpoints para la infraestructura de TI del Ministerio.

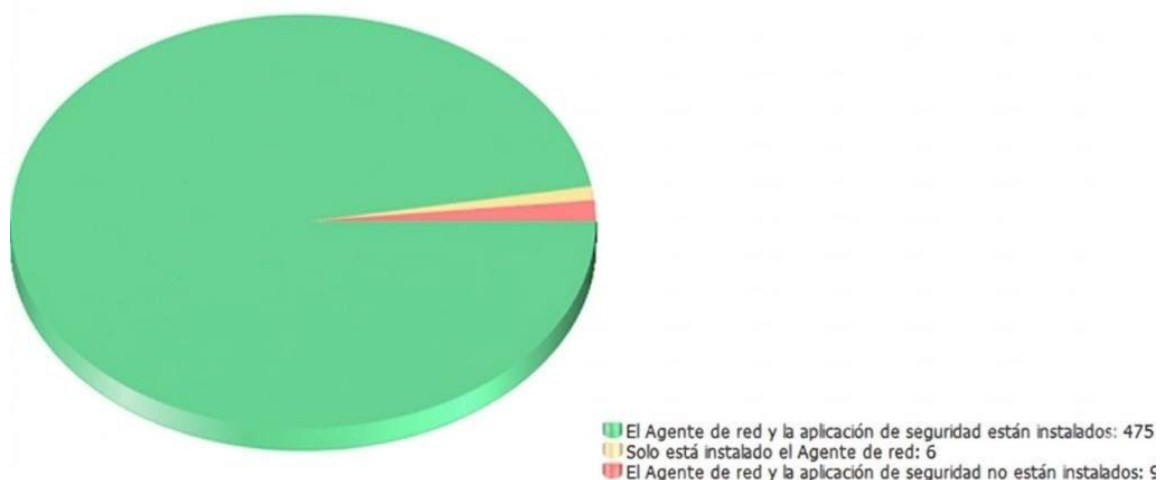


Imagen [13]. Licenciamiento de endpoints para la infraestructura de TI del Ministerio.

- **Gestión de Vulnerabilidades de Software:** Se evidenció una disminución positiva en las vulnerabilidades críticas detectadas en los equipos. En julio se reportaron XXX dispositivos con vulnerabilidades de gravedad crítica, cifra que disminuyó a XXX en el mes de septiembre. Las vulnerabilidades de gravedad alta también bajaron de 97 a 61.

Ministerio de Minas y Energía

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





Imagen [14]. Gestión de vulnerabilidades a partir del escaneo de endpoints.

- **Bloqueo de Amenazas:** En enero se detectaron 7 amenazas en 22 archivos diferentes, mientras que en septiembre se eliminaron 80 registros de amenazas de los dispositivos.

SP-149970-SAF	Hace un día	✓	Si	Dispositivos administrados	1 Crítico
SP-149997-OCI	22/01/2026 12:50:12 p. m.	✓	Si	Dispositivos administrados	1 Crítico
SP-151960-GAI	Hace 22 horas	✓	Si	Dispositivos administrados	1 Crítico
SP-151962-DVE	30/08/2024 5:51:16 p. m.	✓	Si	Dispositivos administrados	1 Crítico
SP-150746-SAF	19/12/2023 3:26:37 p. m.	✓	Si	Dispositivos administrados	1 Crítico
SP-150766-SG	19/12/2023 3:26:37 p. m.	✓	Si	Dispositivos administrados	1 Crítico
SP-150718-GIT	Hace 5 minutos	✓	Si	Dispositivos administrados	1 Crítico/Visible
SP-151641-STH	19/12/2023 3:26:32 p. m.	✓	Si	Dispositivos administrados	1 Crítico
SP-149946-DME	06/02/2026 8:58:59 a. m.	✓	Si	Dispositivos administrados	1 Crítico
SP-150730-STH	19/12/2023 3:26:28 p. m.	✓	Si	Dispositivos administrados	1 Crítico
SP-151577-DEE	19/12/2023 3:26:24 p. m.	✓	Si	Dispositivos administrados	1 Crítico
SP-151553-DH	06/11/2025 8:46:48 a. m.	!	No	Dispositivos administrados	Desconocido
SP-151507-DVM	03/10/2025 9:11:13 a. m.	!	No	Dispositivos administrados	Desconocido

Imagen [15]. Bloqueo de amenazas julio-septiembre en la infraestructura de endpoints del Ministerio,

Nota : si se requiere más información se debe solicitar al oficial de seguridad de la información de la entidad.

4.7 Afinamiento de la ciberseguridad

El informe de afinamiento trimestral de la infraestructura perimetral confirma operación normal del clúster en alta disponibilidad, con consumo de memoria entre 51 % y 58 %, CPU entre 17 % y 32 % y sesiones concurrentes dentro de la capacidad descrita por el equipo técnico. Se verificó el estado del clúster, se revisaron procesos con mayor consumo y se mantuvo la versión estable definida para la plataforma. Por razones de publicación no se reproducen seriales, nombres de nodos, interfaces ni direccionamientos.

Entre las acciones ejecutadas se encuentran la depuración de usuarios locales y VPN que ya no se utilizan, el bloqueo de indicadores de compromiso y direcciones asociadas a intentos de ataque, la revisión de políticas de tráfico y la continuidad del monitoreo de conexiones anómalas. El informe también recomienda mantener análisis de vulnerabilidades antes de publicar aplicaciones en Internet y realizar el siguiente mantenimiento preventivo en octubre, además de gestionar oportunamente la renovación del licenciamiento de la plataforma.

El resultado del trimestre muestra que el afinamiento no debe entenderse como una actividad aislada, sino como un control recurrente que articula disponibilidad, mínimo privilegio, reducción de superficie de ataque, respuesta a inteligencia de amenazas y gestión de cambios. Para mejorar la trazabilidad del SGSI se recomienda que cada afinamiento trimestral incluya una matriz de “acción – motivo – evidencia – riesgo mitigado – control ISO/MSPI asociado”.

Tabla 7. Actividades de afinamiento realizadas — T3 2026

Actividad	Estado	Efecto de seguridad
Verificación de HA y capacidad de recursos	Completado	Confirma redundancia y operación dentro de rangos reportados.
Depuración de usuarios locales y VPN	Completado / continuo	Reduce exposición por cuentas huérfanas o innecesarias.
Bloqueo de IoC y conexiones anómalas	Continuo	Fortalece prevención y respuesta frente a amenazas activas.
Revisión y depuración de políticas de tráfico	Continuo	Reduce reglas obsoletas y complejidad operativa.
Mantenimiento preventivo	Programado	Sostiene disponibilidad, soporte y actualización de la solución.
Análisis previo a publicación de aplicaciones	Recomendación permanente	Reduce exposición de vulnerabilidades en servicios publicados.

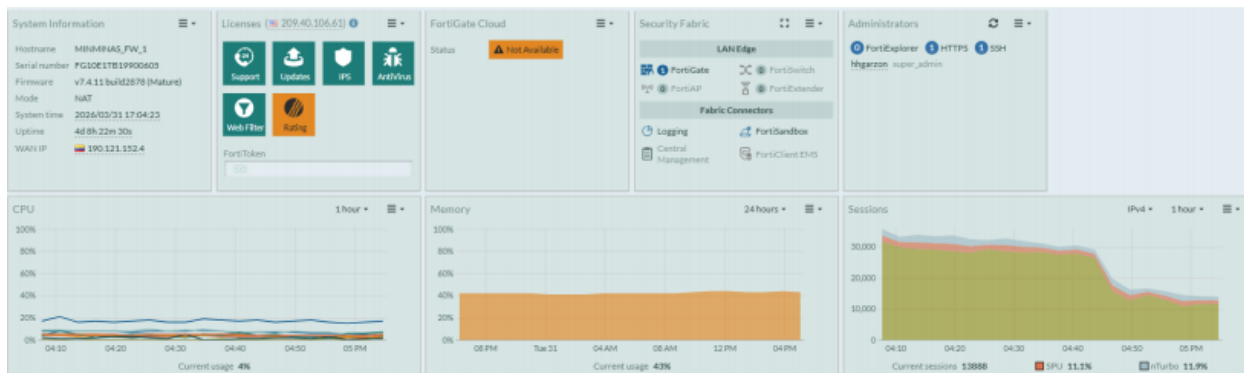


Imagen [16]. Consumo de memoria y CPU tercer trimestre 2026

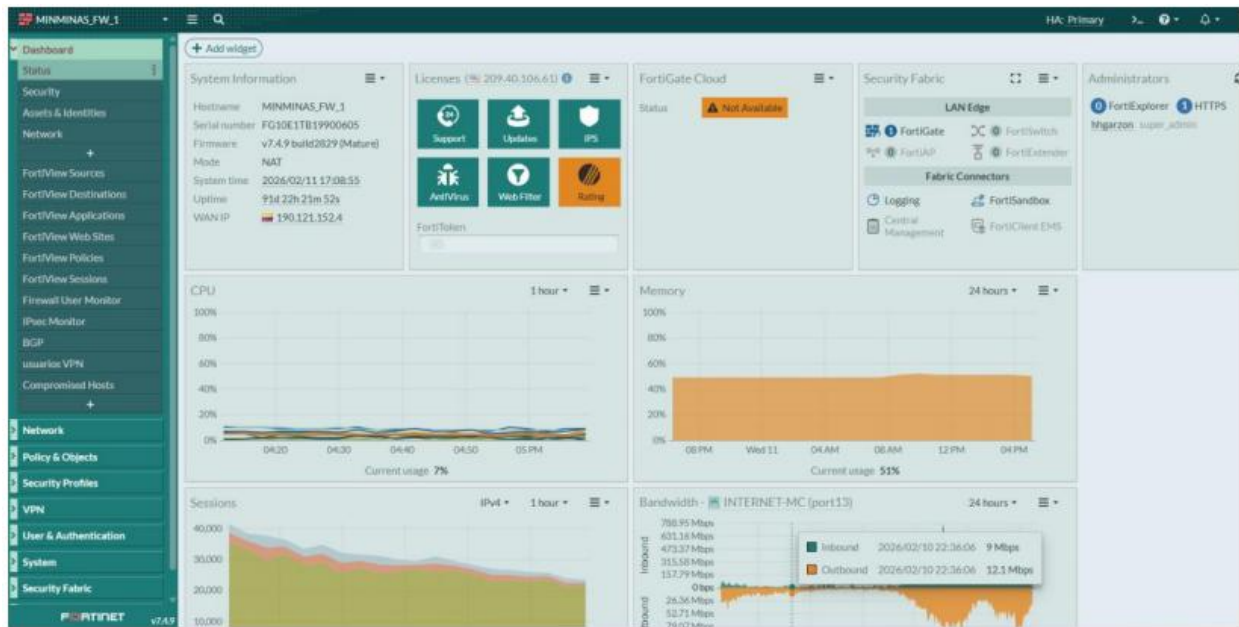


Imagen [17]. Bloqueo de amenazas tercer trimestre 2026

FortiGate 1100E									
MINMINAS_FW_1 (Primary)									
Refresh	Edit	Pin interface faceplate	Remove device from HA cluster						
Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput		
Synchronized	200	MINMINAS_FW_1	FG10E1TB19900605	Primary	4d 8h	12,307	504.87 Mbps		
Synchronized	150	MINMINAS_FW_2	FG10E1TB21900277	Secondary	4d 7h	0	59.00 kbps		

Imagen [18]. Estado HA del cluster tercer trimestre 2026

Ministerio de Minas y Energía

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

4.9 Gestión de vulnerabilidades

La gestión de vulnerabilidades del trimestre se evidencia principalmente a través del informe de seguimiento a lineamientos y prácticas de desarrollo de software y de los controles perimetrales. En el caso de la Ventanilla Única de Trámites (VUT), se documenta un esquema de pruebas que contempla pruebas unitarias, funcionales, integraciones, seguridad, carga/estrés y regresión. La captura de resumen de análisis de vulnerabilidades incluida en el informe muestra cero hallazgos críticos y cero altos para el escaneo referenciado; no obstante, esta evidencia corresponde a un sistema puntual y no debe extrapolarse a la totalidad de la entidad.

El seguimiento documenta además un flujo DevOps/DevSecOps que utiliza control de versiones, revisión de cambios, automatización CI/CD, análisis de vulnerabilidades en imágenes, almacenamiento/versionamiento de artefactos y despliegue separado sobre ambientes de QA y producción. El propio informe advierte que la cobertura de estas prácticas debe validarse por sistema y que es necesario mantener trazabilidad extremo a extremo entre requerimiento, commit, revisión, pipeline, artefacto y versión desplegada.

Flujo DevOps / DevSecOps evidenciado en el seguimiento



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

Imagen 19. Flujo DevOps/DevSecOps documentado para seguimiento.

Fuente: elaboración propia con base en el Informe de Seguimiento a Lineamientos y Prácticas de Desarrollo de Software, T3 2026.

Se identifica una oportunidad de mejora adicional en pruebas de carga y estrés: deben definirse previamente volúmenes, concurrencia, duración, umbrales y criterios de aceptación. Sin estos parámetros, la ejecución de una herramienta de carga genera datos técnicos, pero no permite concluir objetivamente si el rendimiento cumple con el nivel esperado. Para vulnerabilidades, el mismo principio aplica: los escaneos deben asociarse a criterios de severidad, tiempo de remediación, evidencia de cierre y retest.

Tabla 9. Estado de gestión de vulnerabilidades — T3 2026

Ministerio de Minas y Energía

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

Componente	Evidencia T3	Estado	Acción siguiente
Escaneo de aplicaciones	Resumen de análisis de vulnerabilidades de VUT.	Evidenciado para caso puntual	Consolidar cobertura por sistemas priorizados.
DevSecOps	GitLab, Merge Request, Jenkins, Trivy, Registry/Nexus, Kubernetes.	Parcial avanzado	Validar aplicación y temporalidad por proyecto.
Pruebas no funcionales	Pruebas de carga documentadas.	Parcial	Definir umbrales y criterios de aceptación previos.
Remediación y retest	Lineamientos definidos.	Por fortalecer	Relacionar hallazgo, responsable, fecha, cierre y retest.

4.10 Comunicaciones de seguridad de la información

La estrategia de comunicaciones se evidencia a través de piezas de divulgación asociadas a las tres jornadas de capacitación del trimestre. Las piezas incluyeron convocatoria, temática, fecha, hora y medio virtual, permitiendo que la sensibilización se mantuviera integrada a los canales institucionales. La evidencia demuestra una comunicación recurrente y alineada con temáticas de continuidad, protección de información e inteligencia artificial.

Para fortalecer el plan de comunicaciones se recomienda diferenciar indicadores de “difusión” y “apropiación”. El primero puede medirse mediante número de piezas, alcance del canal o visualizaciones; el segundo debe medirse a través de asistencia, respuestas a evaluación, incidentes reportados, resultados de campañas simuladas y cambios observables en comportamientos de seguridad.

Tabla 10. Comunicaciones asociadas a sensibilización T3

Mes	Tema divulgado	Canal / modalidad	Resultado observable
Julio	Seguridad de la información y continuidad del negocio	Virtual / pieza de convocatoria	54 personas registradas.
Agosto	Protección de información confidencial y datos	Virtual / pieza de convocatoria	58 personas registradas.
Septiembre	Inteligencia artificial: ¿aliado o amenaza?	Virtual / pieza de convocatoria	83 personas registradas.

4.11 Capacitación y sensibilización

Durante julio, agosto y septiembre se ejecutaron tres espacios virtuales de capacitación y sensibilización. El informe consolidado documenta materiales pedagógicos, piezas de

Ministerio de Minas y Energía

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

divulgación, participantes y evaluaciones mediante Microsoft Forms. Esta evidencia mejora significativamente la trazabilidad frente a trimestres anteriores, porque permite medir no solo la realización de la actividad sino también la respuesta de los participantes y su desempeño en los cuestionarios.

En julio se registraron 54 participantes y se recibieron 34 respuestas a un quiz de seis preguntas, con puntuación media de 96,1. En agosto se registraron 58 participantes y 22 respuestas a un quiz de cinco preguntas, con media de 90,9. En septiembre se registraron 83 participantes y 55 respuestas a un quiz de cinco preguntas, con media de 79,3. Las tasas aproximadas de respuesta fueron 63,0 %, 37,9 % y 66,3 %, respectivamente. La disminución del resultado medio en septiembre debe analizarse como oportunidad para reforzar el contenido de IA y seguridad, sin asumir por sí sola una disminución general de la cultura institucional.

El siguiente ciclo debe complementar estos indicadores con preguntas comunes que permitan comparar tendencias, segmentación por tipo de usuario y medición posterior. Asimismo, el riesgo transversal de cultura contempla ejercicios simulados o señuelo; no se aportó evidencia de un ejercicio de este tipo durante T3, por lo que permanece como actividad pendiente de demostrar.

Tabla 11. Resultados de capacitación y sensibilización — T3 2026

Mes	Tema	Registrados	Respuestas quiz	Puntuación media	Tasa respuesta
Julio	Hablemos sobre seguridad en la información	54	34	96,1	63,0 %
Agosto	Seguridad de la información para proteger los datos	58	22	90,9	37,9 %
Septiembre	Inteligencia artificial: ¿aliado o amenaza?	83	55	79,3	66,3 %

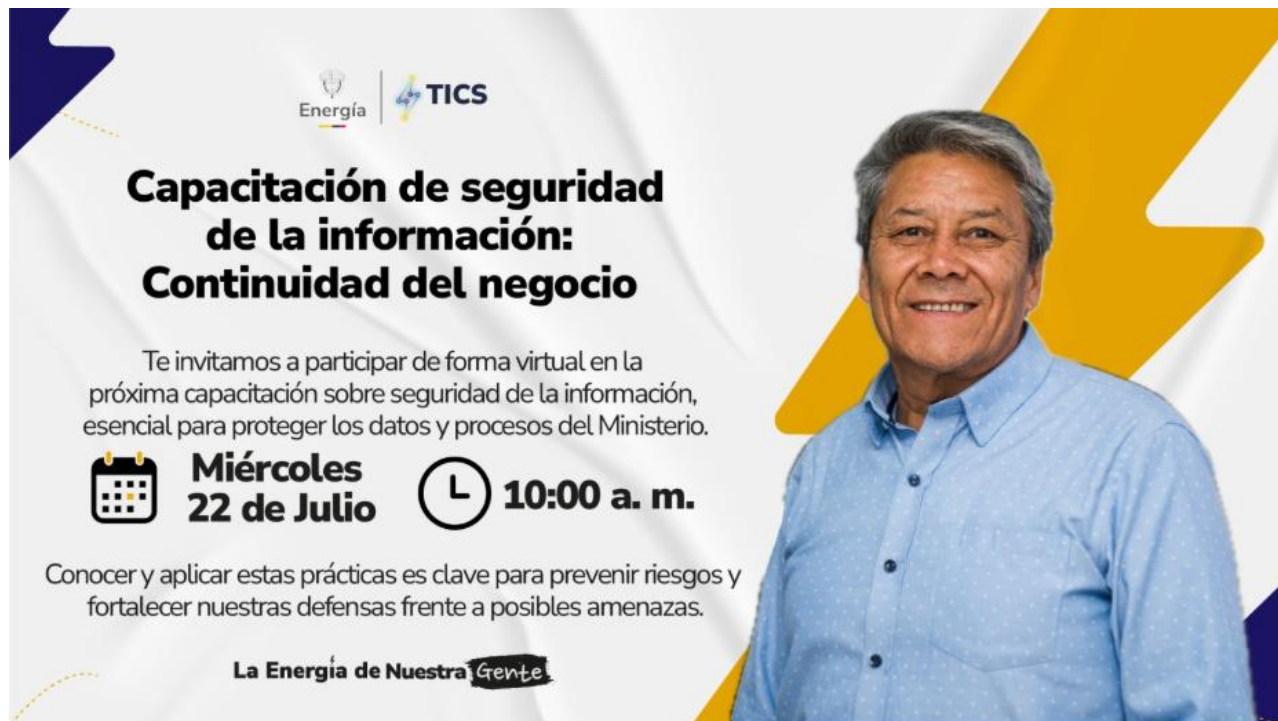


Imagen [20]. Pieza de invitación capacitación: “continuidad del negocio”



Imagen [21]. Pieza de invitación capacitación : “Que nadie vea tu información personal”

Ministerio de Minas y Energía

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



Imagen [22]. Pieza de invitación capacitación : “IA: ‘aliado o amenaza”

4.12 Continuidad, recuperación y gestión de escenario de crisis

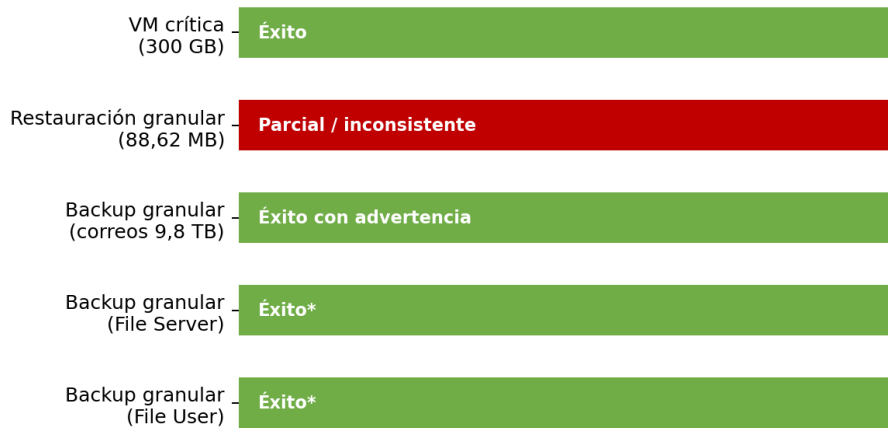
El Plan 2026 programó actividades de preparación y ejecución de un escenario de crisis durante el tercer trimestre. Las evidencias recibidas demuestran capacidad técnica de recuperación mediante restauración de una máquina virtual crítica y ejercicios granulares de backup/restauración, pero no contienen un informe de simulación integral del escenario de crisis, acta de evaluación o evidencia de conmutación al CDA. Por tanto, el seguimiento reconoce los avances técnicos sin equiparlos a la ejecución completa del ejercicio programado.

La restauración de una máquina virtual crítica de aproximadamente 300 GB reportó un tiempo de 3 minutos y 2 segundos entre inicio y finalización y confirmó integridad del punto de recuperación. A su vez, la restauración granular de un conjunto de archivos terminó en aproximadamente 3 minutos y 25 segundos, pero el propio informe concluye que no se recuperó la totalidad de la información. Este contraste es valioso: demuestra que las pruebas periódicas permiten detectar fallas que no serían visibles con el solo indicador de “backup exitoso”.

Ministerio de Minas y Energía

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

Resultados de pruebas de respaldo y restauración aportadas - T3 2026



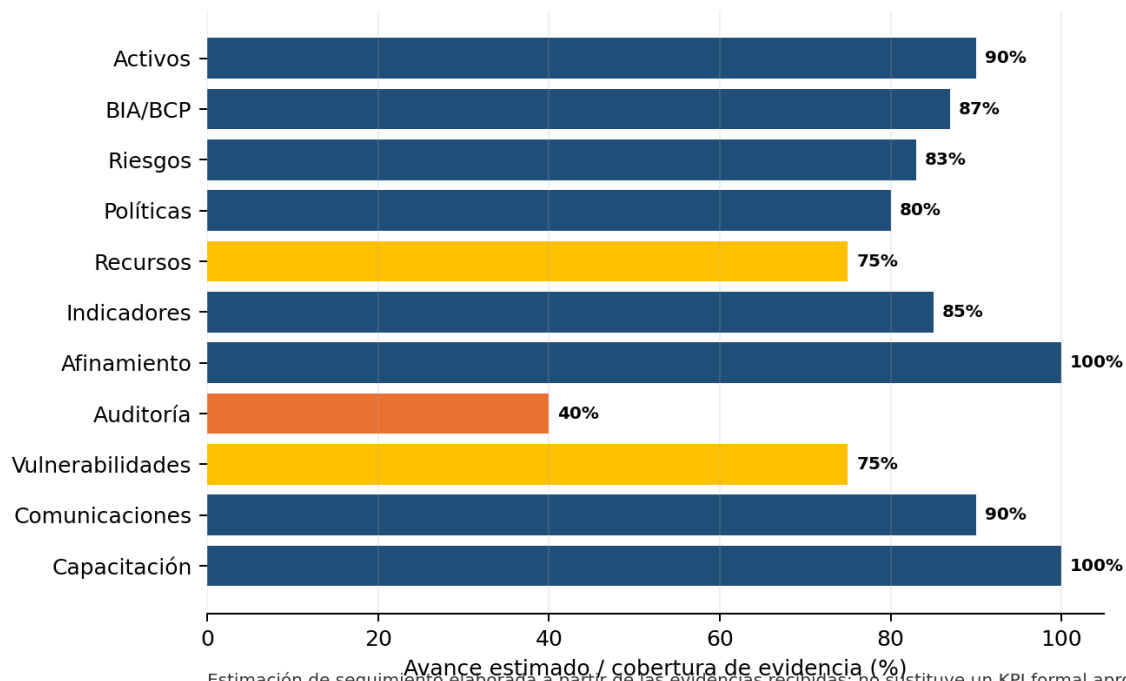
* Los informes de backup granular contienen inconsistencias de fecha/duración que deben corregirse documentalmente.

Imagen 23. Resultado resumido de pruebas de backup y restauración aportadas para el T3.

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

CONSOLIDACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Consolidación estimada del PSPI - tercer trimestre 2026



Estimación de seguimiento elaborada a partir de las evidencias recibidas; no sustituye un KPI formal aprobado.

Ministerio de Minas y Energía

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

Imagen 24. Consolidación estimada del cumplimiento/cobertura de evidencia del PSPI al cierre del T3.

Fuente: elaboración propia. Los porcentajes son estimaciones de seguimiento y no sustituyen indicadores formalmente aprobados.

Tabla 12. Consolidado ejecutivo del Plan de Seguridad y Privacidad de la Información — T3 2026

Componente	Estado T3	Avance estimado T3	Resultado / evidencia	Pendiente Q4
Gestión de activos	En curso avanzado	90 %	Inventario tecnológico actualizado; sin evidencia de cierre formal de matriz.	Publicar versión oficial y conciliar inventarios.
BIA / BCP	En curso avanzado	87 %	Recepción 87 %; matriz maestra e informe institucional en elaboración.	Cerrar pendientes y aprobar guía.
Tratamiento de riesgos	En ejecución	83 %	Avances en R5, R11, R14, R21 y cultura; R23 mantiene brecha DRP.	Cerrar pruebas, evidencia y planes pendientes.
Políticas y procedimientos	En seguimiento	80 %	Se evidencia aplicación de controles existentes.	Formalizar pendientes y matriz de vigencia documental.
Recursos de seguridad	En operación	75 %	Perímetro, backup, VPN y activos operativos.	Aportar evidencia de presupuesto/renovaciones y continuidad integral.
Indicadores	En consolidación	85 %	Disponibilidad, backups, restauración, BIA/BCP y capacitación medidos.	Homogeneizar fuentes y tablero ejecutivo.
Afinamiento de ciberseguridad	Cumplido T3	100 %	Afinamiento trimestral y acciones preventivas ejecutadas.	Mantener mantenimiento y renovación.
Plan de auditorías	Pendiente de evidencia	40 %	No se aportó soporte suficiente de hitos programados.	Anexar informe/actas o formalizar reprogramación.

Ministerio de Minas y Energía

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

Componente	Estado T3	Avance estimado T3	Resultado / evidencia	Pendiente Q4
Vulnerabilidades	Parcial avanzado	75 %	DevSecOps y análisis puntual evidenciados.	Cobertura institucional, cierre y retest.
Comunicaciones	Ejecutado	90 %	Piezas y convocatorias asociadas a tres espacios.	Medir alcance y apropiación.
Capacitación y sensibilización	Cumplido T3	100 %	Tres sesiones con evaluación de conocimientos.	Reforzar temas con menor desempeño y ejercicios simulados.