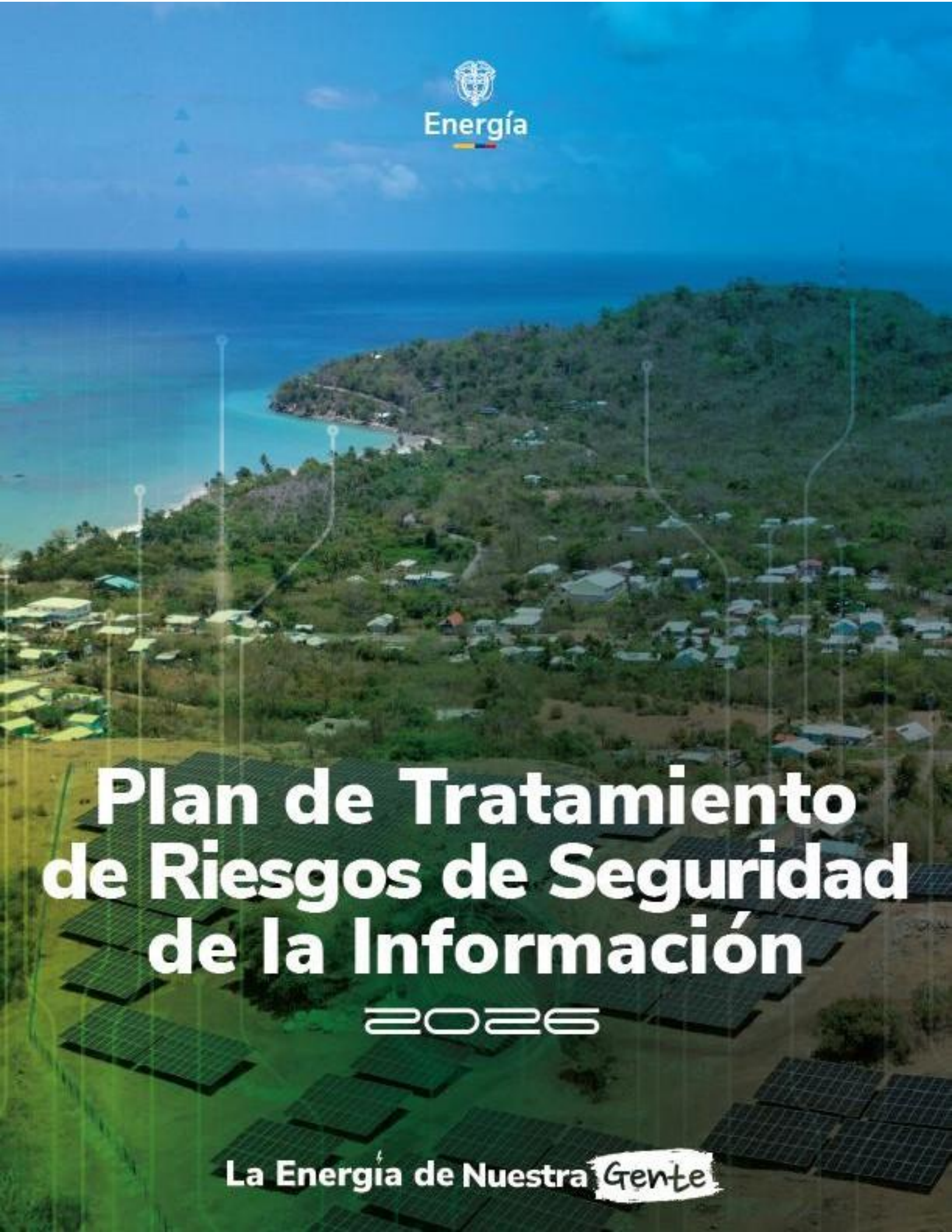
Energía
Plan de Tratamiento de Riesgos de Seguridad de la Información
2026
La Energía de Nuestra Gente

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

Segundo Trimestre 2026

Elaboró:

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

Jimmy Andrés Castellanos Carrillo

Oscar Fabian Ramirez Torres

Oscar Sanchez Sanchez

Andrés Camilo Molano Mendieta

Entidad:

Ministerio de Minas y Energía

Bogotá, 24 de Junio de 2026

CONTENIDO

Tabla de contenido

1. PROCESO

Gestión tecnológica

2. RESPONSABLE DEL PROCESO

Grupo de Tecnologías de la Información y las Comunicaciones
Ing. Jimmy Andrés Castellanos Carrillo
Coordinador Grupo
jacastellanos@minenergia.gov.co
Teléfono: (+57) 6012200300 Ext. 2408

3. OBJETIVO

Documentar el seguimiento y evaluación del Plan de Tratamiento de Riesgos de Seguridad de la Información correspondiente al primer trimestre de 2026 del Ministerio de Minas y Energía (MINENERGÍA). Este seguimiento evalúa el estado de avance de los controles y actividades definidas para los riesgos prioritarios identificados en el plan vigente, a saber: R5 (fallas de seguridad en el ciclo de desarrollo e implementación de IA), R14 (gestión integral de respaldos y pruebas de restauración), R21 (clasificación de activos de información, BIA y BCP actualizados), R23 (gestión de continuidad y DRP soportado en el nuevo CDA/CMS) y el riesgo transversal de Cultura e Identidades Digitales.

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.

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

4.1 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 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.
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.

Riesgo	Conclusión
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.
R23 – Continuidad del negocio y DRP (CDA/CMS)	Se avanzó en la evaluación de alternativas de colocation 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
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,

		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
N° 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).
N° 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.
Cultura e identidades	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.

5. SEGUIMIENTO PLAN DE GESTIÓN

En cumplimento con el plan de tratamiento de riesgos de seguridad de la información se tiene el siguiente resumen que indica la 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 mismo Tabla 3. Acciones de seguimiento y cumplimento para cada uno de los riesgos mapeados para el primer trimestre

Tabla 3

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

No	Reporte Segundo Trimestre
R5	Se documentaron controles de seguridad para proyectos de IA; los dos modelos reportan avance del 100 %. Se realizó hardening del WAF, actualización de versión, limpieza de políticas, depuración de usuarios locales/VPN y bloqueo de IPs maliciosas.
R11	El FortiGate opera en HA, con logs hacia FortiAnalyzer, FSSO funcional contra Directorio Activo, revisión de consumo de canales y reporte VPN SSL del trimestre.
R14	Se concluyó configuración de planes en Veeam 13.01.180 con licencia para 100 nodos. En Arcserve se pausaron 63 servidores y continúan 134 en planes UDP. Las pruebas de restauración granular evidenciaron fallas de consistencia.
R21	Se actualizaron y formalizaron los formatos BIA y BCP; la guía metodológica, la matriz maestra BIA y el informe consolidado se encuentran en revisión.
R23	WAF y MINMINAS-FAZ reportan 100 % de disponibilidad en mayo. Los enlaces de Capital Investments muestran recuperación de mayo frente a abril; persiste necesidad de prueba integral DRP.

No	Reporte Segundo Trimestre
R25	Se observan actividades de depuración de usuarios locales y VPN, así como reporte de intentos fallidos VPN SSL. Frente a la capacitación y sensibilización de seguridad de la información se establece según el cronograma y dándole cumplimiento a los 3 espacios de información referentes, en donde sus temáticas fueron : herramientas contra ciberataques, conceptos clave de seguridad de la información y ciberseguridad y ataques mas comunes y defensa de protección de los datos.

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

El riesgo R5 aborda vulnerabilidades derivadas de prácticas de desarrollo inseguro, ausencia de lineamientos formales para el uso de inteligencia artificial, exposición de datos personales o sensibles, uso de fuentes de datos no controladas y falta de trazabilidad sobre modelos, código, APIs y datasets. Durante el segundo trimestre, el seguimiento se nutre de dos líneas de evidencia: el informe de seguridad del proyecto de IA y el informe de afinamiento FortiGate/WAF.

En el componente de IA, el proyecto “Desarrollo de Modelos de Inteligencia Artificial para el Sector Minero Energético Colombiano” registra dos modelos con avance reportado del 100 %. El Modelo I, asociado al monitoreo del despacho y precios del mercado mayorista de energía, se encuentra en fase intermedia de madurez técnica bajo metodología CRISP-DM, con extracción, filtrado por versión, modelo baseline y validación. El Modelo II, relacionado con transición energética, mapa territorial, EnergyBot y FondoEnergIA, se encuentra en fase de diseño conceptual y arquitectura, con definición de requerimientos funcionales, no funcionales, gobernanza y trazabilidad de datos.

Los controles documentados para este frente incluyen autenticación multifactor, autorización basada en roles, ambientes aislados, acceso controlado a datos sensibles, cifrado de extremo a extremo, versionado criptográfico, anonimización, cadena de custodia, logging detallado de interacciones, inventario de datasets, defensa contra ataques adversarios, filtros de entrada, protección contra extracción de modelos, rate limiting en APIs, ofuscación, validación de fuentes y protección contra envenenamiento de datos. Esta cobertura demuestra que el riesgo R5 ya no se atiende únicamente desde desarrollo seguro tradicional, sino desde un ciclo de vida ampliado para IA, datos, APIs, modelos y gobernanza.

En el componente de seguridad perimetral, el informe de afinamiento evidencia que el FortiGate maestro opera normalmente, con consumo de memoria cercano al 52 %, CPU del 9 %, firmware 7.4.11 y operación en alta disponibilidad. Adicionalmente, se realizó hardening sobre el WAF, garantizando que las políticas cuenten con perfil de protección web personalizado, no se encuentren en modo monitor y tengan política AntiDDoS activa. También se verificaron y eliminaron políticas sin uso, se actualizó el WAF de la versión 7.4.10 a la 7.4.12 y se ejecutó depuración de usuarios locales y VPN no utilizados.

Estos controles reducen la probabilidad de explotación de vulnerabilidades en aplicaciones publicadas, fortalecen la trazabilidad de cambios y disminuyen la exposición asociada al desarrollo e implementación de soluciones de IA. Sin embargo, el cierre total del riesgo requiere formalizar lineamientos de IA institucionales, integrar revisiones de código seguro recurrentes y mantener evidencias de pruebas de seguridad sobre APIs, modelos, datasets y aplicaciones críticas.

Actividad 2026	Periodo	Estado T2 2026	Evidencia
Actualizar metodología de desarrollo seguro incorporando IA y datos personales sensibles	T1 - T2	En curso	Informe de seguridad IA documenta controles para acceso, cifrado, trazabilidad, datasets y defensa frente a amenazas de IA.
Estructurar lineamientos y políticas de uso, desarrollo e implementación de IA	T1 - T2	En curso	Se cuenta con marco de gobernanza, ética y controles; falta evidencia de acto formal o publicación institucional de política definitiva.
Definir y aplicar revisión de código seguro y configuración	T1 - T3	En curs	El proyecto IA reporta repositorios, versionamiento y validación; se recomienda anexar checklist OWASP y evidencia de code review.
Mantener afinamiento de infraestructura de seguridad perimetral	Trimestral	Completado T2	FortiGate estable, WAF actualizado, políticas endurecidas, depuración de políticas y bloqueo de amenazas.
Realizar revisiones periódicas sobre aplicaciones críticas y APIs	Permanente	En curso	Requiere consolidar cronograma y evidencias de pruebas de vulnerabilidad antes de publicaciones en internet.

Las evidencias muestran un cambio de enfoque: de controles centrados en infraestructura hacia controles de seguridad para IA, datos y modelos. Se destacan la trazabilidad de fuentes oficiales, el versionamiento obligatorio de datos, la validación y backtesting, la adopción de software libre y código abierto, y la migración a infraestructura del MME como medidas de soberanía tecnológica y reducción de dependencias externas.

El riesgo residual se mantiene en nivel controlado pero no cerrado. La razón principal es que los controles deben pasar de ser documentación técnica de proyecto a lineamientos institucionales integrados al SGSI, con responsables, periodicidad de revisión, criterios de aprobación, evaluación de privacidad, gestión de sesgos, monitoreo en producción y respuesta ante incidentes de IA

5.2 Riesgo R11: Auditoría y Monitoreo de Sistemas de Información

El FortiGate se encuentra configurado para almacenar logs en un FortiAnalyzer con IP XXXXXXX, lo que permite conservar trazabilidad de eventos y generar reportes de tráfico. Adicionalmente, se verificó el uso del agente FSSO con estado funcional contra el servidor XXXXXX, permitiendo identificar usuarios y configurar permisos de navegación asociados a identidad. Esta relación entre logs, identidad y navegación fortalece la capacidad de auditoría y análisis posterior ante eventos anómalos.

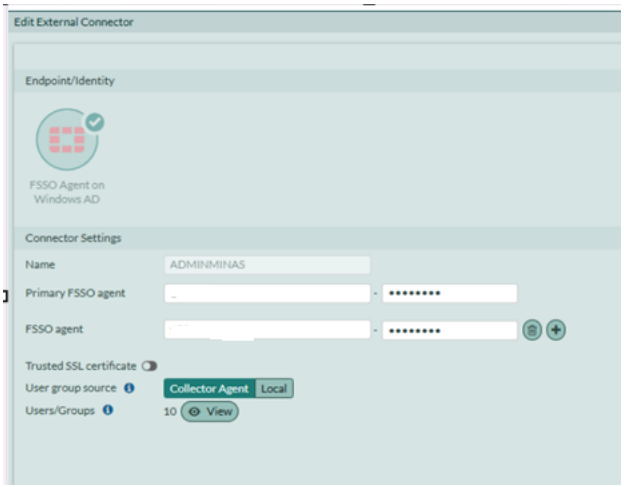

Imagen 1. FSSO activo y configurado con los logs de fortianalyzer.

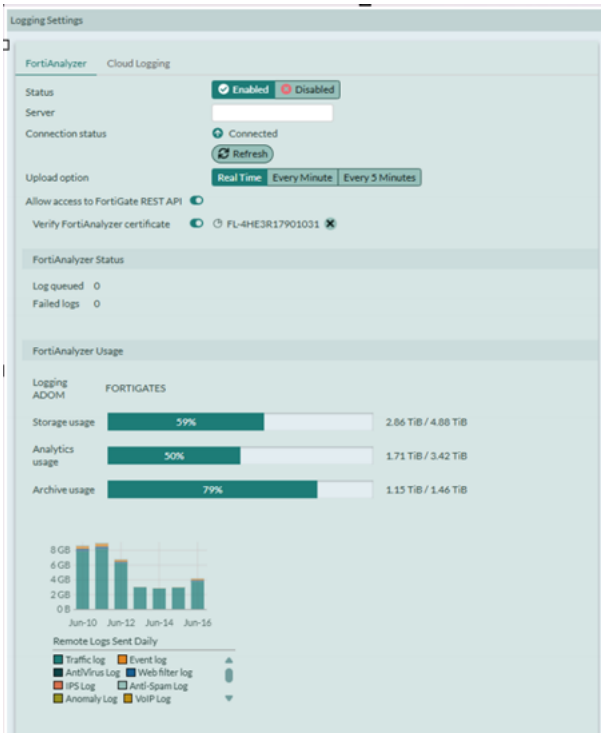

Imagen 2. Configuración de fortigate.

El informe también indica que no se evidencia saturación de canales o interfaces. A nivel de acceso remoto, el reporte VPN SSL del trimestre cubre el periodo 1 de abril a 18 de junio de 2026, incluyendo número de conexiones, duración agregada, volumen transferido e intentos fallidos. El mayor volumen individual de conexiones registrado en el top del reporte alcanza 325 conexiones y la duración agregada máxima reportada es de XXXXX. En los intentos fallidos, el top de VPN FAIL LOGIN muestra cuentas con 157 y 153 intentos fallidos, seguidas de registros menores de 39, 31, 30 y 29 intentos, lo que requiere seguimiento focalizado sin exponer datos personales en reportes ejecutivos.

La existencia de reportes de VPN, logs perimetrales, FSSO y disponibilidad constituye evidencia de operación del control de monitoreo. No obstante, el tratamiento del riesgo R11 debe avanzar hacia una correlación más madura entre intentos fallidos, direcciones IP, horarios, perfiles de usuario, alertas del SOC y acciones correctivas. Esto permitirá diferenciar errores de autenticación, pruebas operativas, credenciales obsoletas, cuentas compartidas, automatización maliciosa o potenciales ataques de fuerza bruta.

La infraestructura genera y concentra evidencia; sin embargo, la madurez del control dependerá de que la información se traduzca en reglas de alerta, casos de uso, revisión de cuentas y acciones documentadas. Los intentos fallidos de VPN SSL deben convertirse en insumo para depuración de identidades, aplicación de MFA, bloqueo adaptativo y campañas de cultura digital.

5.3 Riesgo R14: Gestión Integral de Respaldos y Pruebas de Restauración

El riesgo R14 representa el frente más sensible del segundo trimestre. La evidencia muestra avances importantes en configuración de la plataforma de respaldo, pero también hallazgos críticos en las pruebas de restauración. En seguridad de la información, el respaldo solo se considera un control efectivo cuando permite recuperar información íntegra, dentro de tiempos razonables y bajo procedimientos repetibles.

Durante el segundo trimestre se concluyó la configuración de los planes de backup con Veeam Backup & Replicator versión xxxxx, licenciada con capacidad para XX nodos o servidores. Esta cobertura representa un avance frente a la transición iniciada en el primer trimestre y fortalece la capacidad del Ministerio para respaldar información alojada en servidores físicos y virtuales. El informe técnico señala que, a partir del segundo semestre, se buscará ampliar el licenciamiento para incluir alrededor de XX nuevas licencias y cubrir todos los servidores físicos y virtuales, lo cual resulta fundamental para minimizar riesgos de pérdida de información.

La transición desde Arcserve también avanzó. Se han venido pausando los procesos de backup y respaldo a cintas mediante la funcionalidad UDP para realizar backup a disco dentro de Arcserve. A la fecha del informe, se pausaron aproximadamente XX servidores virtuales y continúan ejecutándose XXX servidores virtuales dentro de planes de backup a disco UDP, con RPO de 6 horas, 24 horas, semanal, mensual y estados apagados. Adicionalmente, el reporte indica ejecución satisfactoria de jobs UDP Arcserve Backup.

No obstante, las pruebas de restauración granular realizadas en junio arrojan resultados no satisfactorios. La restauración granular sobre el servidor XXXXXXX, carpeta XXXXXX, partió de una imagen Veeam Full del XXXXX XXX p.m.; se reportó tamaño por restaurar de XXX MB y tamaño restaurado de XXX KB, con inicio el XXXX a las XXXX a.m. y finalización a las XXXX p.m., para un RTO aproximado de XX horas y XX minutos. El informe concluye que el bloque de datos no es consistente ni funcional.

La segunda prueba, realizada sobre la base de datos SQL XXXXXX en el servidor XXXXXX, partió de una imagen Veeam Full del XXXX XXXX a.m. El ejercicio inició el XXXX a las XXX a.m. y finalizó a las XXX a.m., con tiempo total de XXX minutos; sin embargo, el resultado final fue que no se realizó la restauración y se concluyó que la restauración no es consistente ni funcional. Estos resultados evidencian una brecha crítica entre disponer de backup y poder restaurar de manera confiable

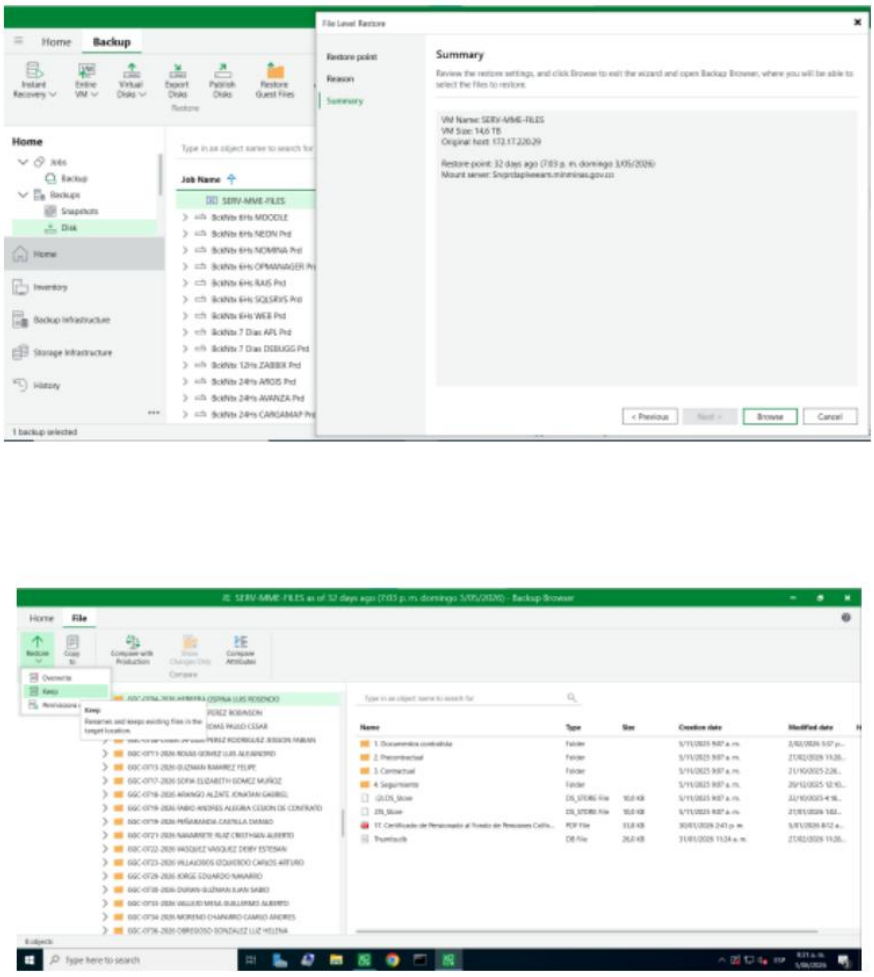

Imagen 3. Herramienta de veam Backup replication, solo corresponde a la imagen de funcionamiento inicial.

La configuración de Veeam y el avance de transición desde Arcserve son logros importantes; sin embargo, el riesgo residual de R14 no puede considerarse bajo porque dos restauraciones controladas no alcanzaron resultados consistentes. En términos de control, esto significa que la disponibilidad de copias de seguridad aún no se traduce plenamente en recuperabilidad comprobada.

Se recomienda mantener el escalamiento con el proveedor Heimcore y el fabricante Veeam, documentar causa raíz, validar compatibilidad con hipervisor, revisar repositorios, cadenas de backup, permisos, cifrado, integridad de puntos de recuperación y ejecutar nuevas pruebas DataLabs hasta lograr restauraciones exitosas, medibles y repetibles. Estas pruebas deben coordinarse con R21 y R23, dado que los RTO/RPO dependen de BIA/BCP y del DRP institucional.

5.4 Riesgo R21: Clasificación de Activos de Información, BIA y BCP Actualizados

El informe de avance del 9 de junio indica que la guía metodológica para la implementación del Análisis de Impacto al Negocio se encuentra en proceso de revisión y actualización, con el objetivo de fortalecer lineamientos institucionales para identificar y valorar procesos críticos, recursos esenciales, impactos, tiempos de recuperación y procesos alternos. La guía está en revisión y validación por parte de la Oficina de Planeación y Gestión Internacional.

En materia de formatos, se actualizaron y formalizaron los instrumentos T-GT-F-84 - Análisis de Impacto al Negocio (BIA) y T-GT-F-85 - Plan de Continuidad del Negocio (BCP). Para el formato BIA, las mejoras incluyen reestructuración de campos, mejor organización de información relacionada con servicios, activos de información, aplicaciones y recursos críticos, y ajuste de instrucciones para asegurar consistencia. Para el formato BCP, se estandarizó la estructura del plan y se alineó con los resultados que serán obtenidos por el ejercicio BIA. Ambos instrumentos fueron gestionados para formalización dentro del Sistema Integrado de Gestión.

También se diseñó una matriz maestra BIA consolidada para integrar la información proveniente de todas las dependencias de la entidad. Esta matriz se encuentra en revisión y validación por parte de la Oficina de Planeación y Gestión Internacional. Finalmente, se estructuró un informe consolidado de resultados BIA para presentar los resultados institucionales a la Oficina de Planeación y Gestión de Proyectos (PMO) y a las instancias de gobierno correspondientes.

Frente al tema de los activos de información y de acuerdo a la procedimiento de gestión de activos de información, esta actividad se encuentra en un 90% , donde hacen falta 8 procesos dentro de la entidad de 61 por la identificación y clasificación de los mismos.

En el tercer trimestre deben definirse responsables por dependencia, cronograma de diligenciamiento, criterios de calidad, revisión de consistencia, versión oficial de matriz e incorporación de resultados al DRP, a los planes de backup y a las pruebas de restauración. El

mayor valor del BIA se logrará cuando sus RTO/RPO se conviertan en parámetros técnicos para Veeam, CDA/CMS y simulacros de continuidad.

5.5 Riesgo R23: Gestión de Continuidad y DRP Soportado en el Nuevo CDA/CMS

El riesgo R23 se relaciona con la capacidad institucional para mantener o recuperar servicios críticos ante fallas de infraestructura, pérdida de datos, ciberataques o indisponibilidad del centro principal. En el segundo trimestre se observan evidencias de continuidad operativa y disponibilidad, pero aún no se identifica una prueba integral que combine restauración, conmutación al CDA y operación de servicios críticos.

En términos de disponibilidad, el componente MINMINAS-FAZ reporta 100 % para múltiples ventanas de medición, incluyendo últimas 4, 6, 8, 12 y 24 horas, últimos 7, 30, 60 y 90 días, este trimestre, trimestre pasado, últimos 3 meses y últimos 6 meses. De forma similar, el reporte de WAF MINENERGIA generado el 14 de junio reporta 100 % para las ventanas incluidas. Estos indicadores son positivos para continuidad operativa y protección de aplicaciones publicadas.

Los reportes de Capital Investments muestran una lectura diferenciada. En abril, cuatro de los cinco enlaces revisados se mantuvieron en niveles cercanos o iguales al 100 %, pero el enlace Cll 43 # 57-31 Centro Administrativo Nacional Item 3 tuvo disponibilidad promedio aproximada de XXX %, con indisponibilidad total entre el 1 y el 9 de abril y XXXX % el 10 de abril. En mayo se evidencia recuperación, con promedios superiores a XXX% en los cinco enlaces. Esta mejora indica estabilización, pero la excepción de abril debe quedar documentada como evento a analizar dentro de continuidad y gestión de proveedores.

El reporte VPN SSL también aporta evidencia para R23, en la medida en que el acceso remoto seguro es un componente de operación en contingencia y soporte técnico. Se recomienda usar las métricas de conexión, duración, transferencia e intentos fallidos como insumo para definir perfiles de acceso durante escenarios de DRP, listas de usuarios críticos, cuentas de proveedores y mecanismos de control reforzado para tareas de recuperación.

5.6 R25. Riesgo Transversal: Cultura de Seguridad Digital y Gestión de Identidades (Contraseñas y MFA)

Durante el primer trimestre se reportó la obligatoriedad de MFA en Microsoft 365 y la estructuración de la Política de Gestión de Identidades y Autenticación. Para el segundo trimestre, las evidencias recibidas se concentran principalmente en controles técnicos relacionados con depuración de usuarios locales y VPN, monitoreo de accesos VPN SSL, registro de intentos fallidos y mantenimiento de controles perimetrales. El informe de afinamiento señala que se realizó depuración de usuarios locales y de VPN que ya no se utilizan, lo cual reduce exposición por cuentas huérfanas o innecesarias.

El reporte VPN SSL del periodo 1 de abril a 18 de junio permite identificar usuarios con intentos fallidos de autenticación y una tendencia de uso del acceso remoto. En un informe ejecutivo, estos datos deben tratarse como información sensible y utilizarse para acciones de seguimiento,

no para exposición innecesaria de identificadores personales. La lectura de seguridad recomienda generar una lista interna controlada de cuentas con intentos fallidos altos, validar si corresponden a errores de usuario, ataques automatizados, credenciales vencidas, cuentas de proveedor o intentos sospechosos, y aplicar medidas de remediación.

Frente a la capacitación y sensibilización, se generaron según el cronograma del plan de seguridad y privacidad de la información 3 sesiones enfocadas en capacitar al personal interno del Ministerio en herramientas de ciberseguridad, conceptos de protección de datos , información y de conocimiento en nuevos ataques en lo concerniente a tácticas y técnicas de las ciberdelincuentes, para la protección de los activos de información de la entidad.

Avance y consolidación de tareas del plan de tratamiento de riesgos de seguridad de la información

Riesgo	Actividades Programadas (Q2 - Meses 4, 5, 6)	Evidencia de Ejecución en el Segundo Trimestre	Avance Estimado (Q2)	Avance según totalidad del plan
R5 - Desarrollo seguro / IA	Act 2: Lineamientos de IA. Act 3: Revisión de código y ambientes seguros.	**Finalizado:** Los Modelos de IA (I y II) reportaron un **100% de avance** en sus fases actuales. Se implementaron ambientes aislados, cifrado y anonimización de datos. Además, se completó el afinamiento trimestral (abril-junio) del firewall Fortigate y el WAF, depurando políticas y bloqueando IPs maliciosas.	**100%**	50%
R14 - Backups y Restauración	Act 1: Procedimientos de respaldo. Act 2: Pruebas de restauración de sistemas críticos.	**Finalizado:** Se configuró la herramienta Veeam Backup & Replicator (v.13) para los servidores. Se ejecutaron las pruebas de restauración granulares en junio (File Server el 5 de junio y Base de Datos SQL el 10 de junio). *(Nota: Las pruebas arrojaron resultados inconsistentes y fallidos, pero la actividad de testeo programada sí se ejecutó al 100%).*	**100%** (En ejecución de metas)	50%

R21 - Activos / BIA / BCP	Act 1: Culminar matriz. Act 2: Actualizar BIA y BCP.	**Parcial:** En el informe de avance de junio de 2026, se reportan como **"Finalizados"** los formatos T-GT-F-84 (BIA) y T-GT-F-85 (BCP). Sin embargo, la Guía de Implementación, la Matriz Maestra Consolidada y el Informe Consolidado continúan **"En revisión"** por parte de la Oficina de Planeación.	**60%**	40%
R23 - Continuidad / DRP	Actualizar DRP con nuevo Centro de Datos Alterno (CDA).	**No Aplica en Q2:** Según el cronograma oficial del plan de tratamiento, las actividades para este riesgo (M7 a M12) inician a partir del tercer trimestre (julio).	**N/A**	**N/A**
R24 - Cultura e Identidades	Act 1, 2, 3: Sensibilización, políticas, uso de MFA y simulacros.	**Continuo:** Es una actividad transversal. Durante el trimestre (abril-junio) se realizó depuración de usuarios de VPN e identidades locales sin uso.	**100%** (Operatividad continua)	50%
AVANCE GENERAL DEL PLAN	**Consolidado del Segundo Trimestre (Q2)**	Promedio del cumplimiento de las metas trazadas específicamente para los meses de abril, mayo y junio.	**43%**	