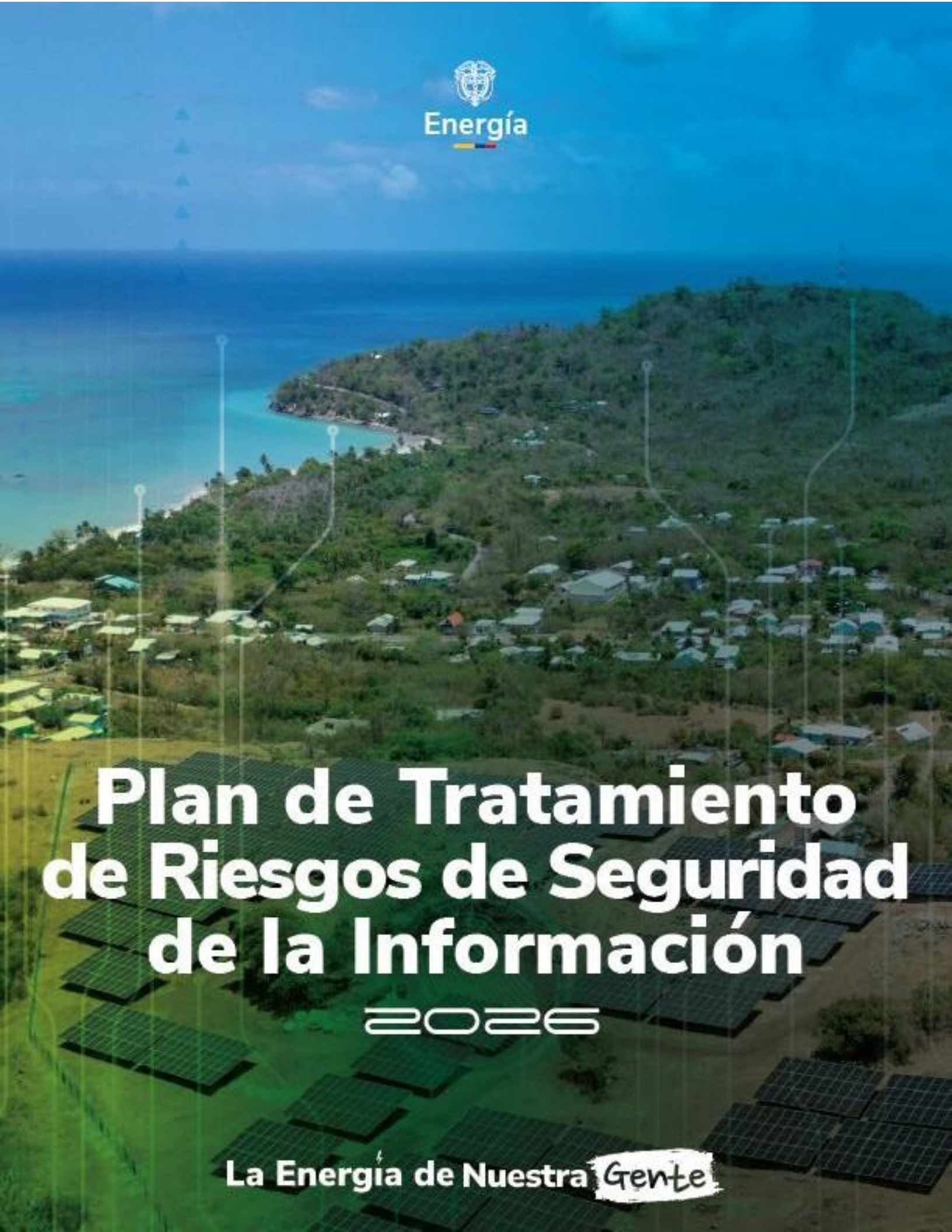
Energía
Plan de Tratamiento de Riesgos de Seguridad de la Información
2026
La Energía de Nuestra Gente

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

Primer 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, 10 de Abril 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.

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 el roadmap 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 primer trimestre plan de tratamientos de riesgos de seguridad de la información- actividades realizadas, primer trimestre.

No	Reporte primer Trimestre
R5	Se afinó la seguridad perimetral actualizando el WAF, depurando políticas y bloqueando IPs maliciosas mediante indicadores de compromiso. Para los modelos de IA, se implementaron ambientes aislados, cifrado, anonimización de datos y defensas técnicas contra el envenenamiento de información.
R1	Se actualizó la herramienta de monitoreo y se consolidó el envío centralizado de logs para garantizar su trazabilidad. Asimismo, se configuró el bloqueo proactivo de amenazas y se verificó el agente FSSO contra el Directorio Activo para auditar la navegación asociada a la identidad de cada usuario.
R14	Se instaló Veeam Backup & Replicator logrando la inclusión inicial de 95 servidores, mientras se ajustaban y pausaban progresivamente los equipos en ArcServe. Se activó la inmutabilidad de los repositorios contra ransomware y se lograron excelentes métricas, como la restauración de 200 GB en 15 minutos.
R21	Se adelantó la segunda fase de capacitación para los delegados asignados en cada dependencia de la institución. Posteriormente, entre febrero y marzo, se llevó a cabo el diligenciamiento inicial de la matriz de activos y comenzó la revisión primaria de dicha información.
R23	Se suscribió y dio acta de inicio al contrato GGC-1755-2026, el cual dotará a la entidad de un nuevo Centro de Datos Alterno y capacidades NOC/SOC. Técnicamente, ya iniciaron las conexiones y trabajos de configuración operativa enfocados en la recuperación ante desastres.

R25	Se configuró y exigió obligatoriamente el doble factor de autenticación (MFA) en Microsoft 365 para todos los usuarios, eliminando el riesgo de la credencial simple. Para formalizar esto, se estructuró la Política de Gestión de Identidades, acompañada de nuevas capacitaciones.

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

El riesgo R5 aborda las vulnerabilidades potenciales derivadas de prácticas de desarrollo inseguro y de la ausencia de lineamientos formales para la incorporación de soluciones de Inteligencia Artificial (IA) en los sistemas de información del Ministerio. Sobre la base del avance logrado en 2025 (que incluyó la consolidación de la metodología de desarrollo seguro en el Manual de Metodología y Arquitectura de Referencia para el Desarrollo de Sistemas de Información, la implementación de pipelines CI/CD en GitLab con validaciones automáticas, y el despliegue de SonarQube con Kubernetes para análisis estático) el Plan 2026 propone profundizar estos controles incorporando el componente de IA y el tratamiento de datos personales sensibles.

Durante el primer trimestre, las actividades más concretas y verificables en el marco de este riesgo corresponden a las acciones de afinamiento de la infraestructura de seguridad perimetral, que constituyen una línea de defensa fundamental frente a las amenazas externas que buscan explotar vulnerabilidades en los sistemas de información publicados en internet. La actualización del XXXX HA a la versión X.X.XX y la realización de actividades de afinamiento del WAF representan controles técnicos directamente vinculados a la reducción de la superficie de ataque sobre las aplicaciones del Ministerio.

De manera específica, la depuración de 7 políticas WAF obsoletas, dejando activas 125 políticas vigentes, la asignación de perfiles de protección web personalizados en 7 aplicaciones que previamente operaban con el perfil predeterminado, la desactivación del protocolo HTTP en las publicaciones de portales institucionales, y el bloqueo de IPs maliciosas con base en indicadores de compromiso (IoC) de Colcert, Csirt y el SOC del Ministerio, son medidas que reducen directamente la probabilidad de materialización de vulnerabilidades en el ciclo de desarrollo y operación de los sistemas de información.

Tabla 4. Estado de actividades — Riesgo R5 T1 2026

Actividad 2026	Responsable	Trimestre	Estado T1 2026
Actualizar metodología de desarrollo seguro incorporando IA y datos personales sensibles	Equipo Seguridad Información	T1 - T2 2026	EN CURSO
Estructuración de lineamientos y políticas de uso, desarrollo e implementación de IA en la entidad	Equipo Seguridad Información	T1 - T2 2026	EN CURSO
Definir e implementar procedimiento de revisión de código seguro (OWASP, checklists, revisiones entre pares)	Equipo Desarrollo / Seguridad	T1 - T2 2026	EN CURSO
Mantenimiento preventivo y actualización FortiGate (firmware, perfiles WAF, depuración políticas)	Equipo Seguridad / Proveedor	T1 2026	COMPLETADO
Bloqueo de IPs maliciosas con IoC (Colcert, Csirt, SOC MME)	Equipo Seguridad / SOC	Permanente	COMPLETADO

Fuente: Grupo TICS — Informe Afinamiento FortiGate T1 2026

Para mitigar el riesgo de exposición de datos sensibles por el uso de IA, se documentaron e implementaron estrictos controles y protocolos en el marco del proyecto "Desarrollo de Modelos de Inteligencia Artificial para el Sector Minero Energético Colombiano", adelantado junto con la Universidad Tecnológica de Pereira (UTP). Las acciones implementadas incluyen:

- **Alineación Normativa y Gobernanza:** Se definió un Marco de Gobernanza y Supervisión de Analítica Avanzada e IA, estableciendo principios de uso ético y responsable (alineados con el Conpes 3975) y cumpliendo con el Paquete P4 de Seguridad y Privacidad del marco IDEC 2.1.
- **Segregación y Control de Accesos:** Se establecieron ambientes aislados para el entrenamiento de los modelos, separados de la infraestructura de producción del Ministerio, reforzados con Autenticación Multifactor (MFA) y autorización por roles (RBAC).
- **Protección y Privacidad de Datos:** Se implementó cifrado End-to-End y técnicas de anonimización sobre los conjuntos de datos de entrenamiento para proteger la información confidencial.

- **Defensa contra Amenazas Específicas:** Se desarrollaron sistemas de detección en tiempo real para ataques adversarios, filtros de entrada inteligentes, técnicas de ofuscación contra ingeniería inversa, y protección contra el envenenamiento de datos (data poisoning).

Riesgo R11: Auditoría y Monitoreo de Sistemas de Información

Durante el primer trimestre de 2026, la mitigación de este riesgo presentó avances significativos tanto en el fortalecimiento de la infraestructura actual (XXXXX) como en la proyección estratégica del monitoreo sectorial:

1. **Centralización de Logs y trazabilidad de eventos :** Para garantizar la trazabilidad de los eventos de red y poder generar reportes detallados de tráfico y seguridad, se verificó y consolidó la configuración del XXXXX para enviar y almacenar todos sus logs de manera centralizada en el servidor (IP XXX.XXX.X.X.). Como parte del mantenimiento de este trimestre, la herramienta fue actualizada de la versión XX.X.X a la versión X.XX.XX (la última versión estable), garantizando así un procesamiento de logs sin interrupciones y con las mejores características de seguridad.

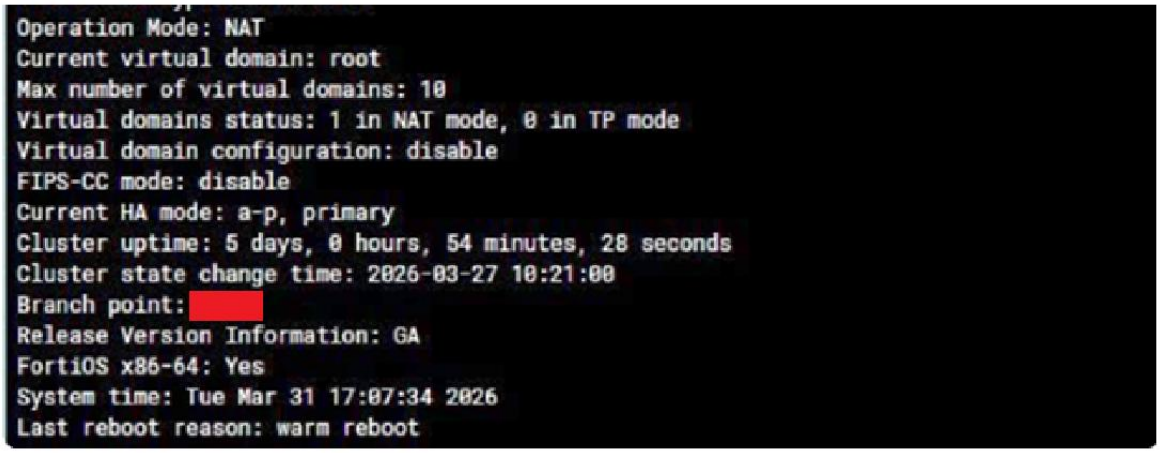

Imagen [1] . Actualización de la herramienta de ciberseguridad para hacer monitoreo de eventos

2. **Monitoreo Proactivo y Bloqueo de Amenazas (Integración SOC/CSIRT):** El sistema de monitoreo perimetral se mantuvo activo recibiendo inteligencia de amenazas. Durante el trimestre, se configuró el bloqueo proactivo de direcciones IP que intentaron ataques contra el Ministerio, así como el bloqueo de Indicadores de Compromiso (IoC) notificados mediante boletines por entidades externas y de control como Colcert, el CSIRT y el propio SOC de la entidad.

3**. Trazabilidad de Identidades (Agente FSSO):** Para asegurar que las auditorías de navegación web estén correctamente asociadas a las identidades de los usuarios, se verificó el estado funcional del agente FSSO (Fortinet Single Sign-On) contra el servidor del Directorio

Activo (XXX.X.X.X.), permitiendo identificar y auditar con precisión a los usuarios y sus permisos de red.

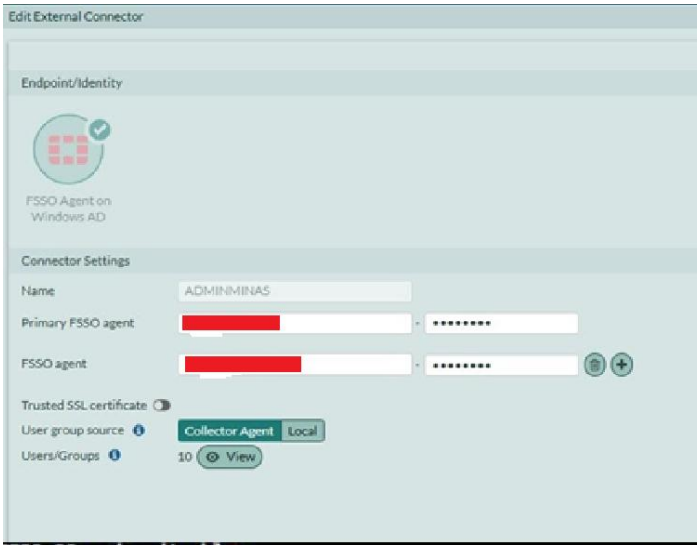

Imagen [2] . Agente FSSO activo

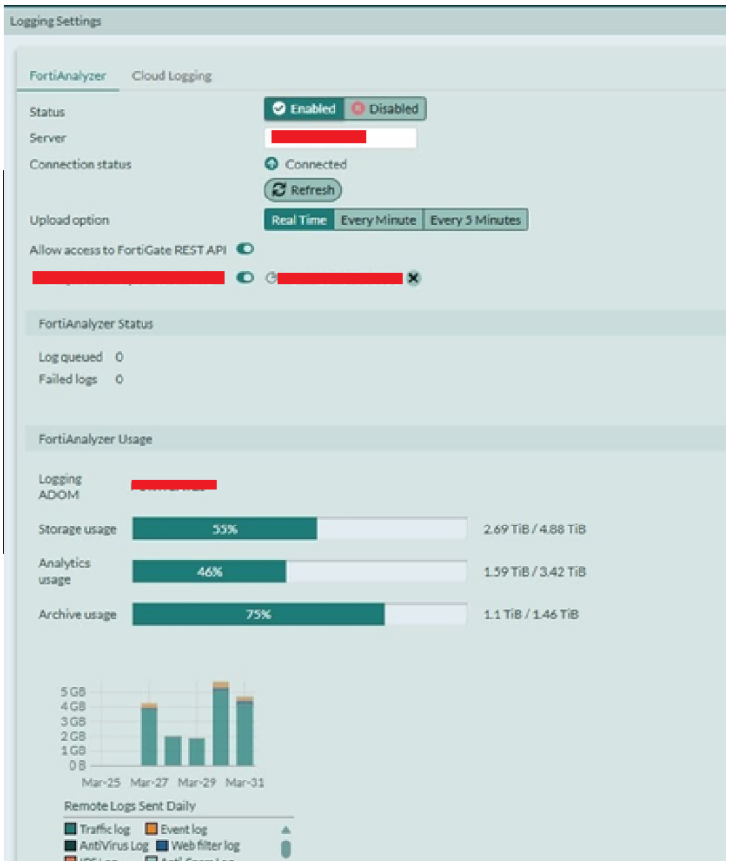

Imagen [3] . Agente FSSO activo

Riesgo R14: Gestión Integral de Respaldos y Pruebas de Restauración

El riesgo R14 representa el área de mayor avance durante el primer trimestre de 2026. El Plan de Tratamiento identificó como actividades prioritarias la elaboración del procedimiento formal de respaldo y restauración, la definición de un programa anual de pruebas de restauración y la alineación de la herramienta de backup con los RTO/RPO definidos en BIA/BCP. En respuesta a estas necesidades, el Ministerio inició la transición hacia una solución de respaldo más robusta y moderna.

Desde enero de 2026 se realizó la instalación y configuración de la herramienta Veeam Backup & Replicator versión XX.X.X.X, adquirida con licenciamiento para XXX nodos. Este cambio tecnológico representa una mejora cualitativa significativa respecto a la herramienta ArcServe UDP utilizada previamente, la cual había presentado fallas operativas y operaba al 80% de su capacidad según el análisis de 2025. Al corte del 24 de marzo de 2026, se han incorporado 95 servidores virtuales dentro de los planes de backup de Veeam, quedando únicamente 5 servidores pendientes de inclusión para completar la cobertura de la licencia actual.

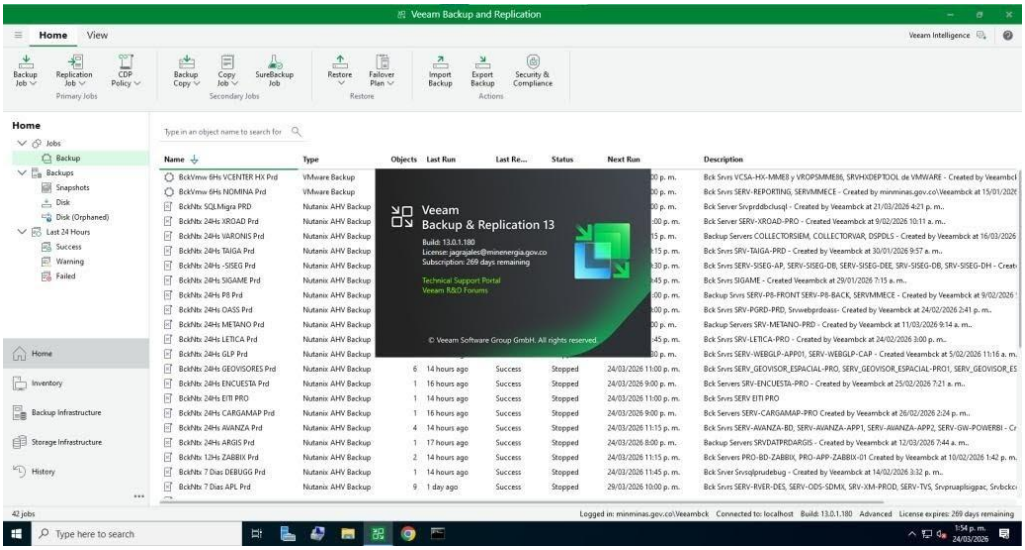

Imagen [4] . Herramienta de veam Backup replication 13, solo corresponde a la imagen de fundionamiento inicial.

Paralelamente, se han intervenido y ajustado 209 servidores virtuales dentro de los planes de backup a disco UDP de ArcServe (con configuraciones de RPO de 6 horas, 24 horas, semanal y mensual), poniéndolos en estado de pausa de manera progresiva a medida que Veeam asume

su cobertura. Este proceso de transición ordenada garantiza que ningún servidor quede sin cobertura de respaldo durante el período de migración.

A pesar del avance significativo en la implementación tecnológica, es importante destacar que el procedimiento formal de respaldo y restauración, así como el programa periódico de pruebas de restauración, se encuentran pendientes de formalización. Estas actividades son críticas para que la cobertura técnica de backup se traduzca en una capacidad real y verificada de recuperación ante incidentes.

Tabla 5. Estado de actividades — Riesgo R14 T1 2026

Actividad 2026	Responsable	Trimestre Planif.	Estado T1 2026
Instalación e implementación de Veeam Backup & Replicator Vxx.x.x.x. (XXX nodos)	Equipo Infraestructura / Seguridad	T1 2026	**COMPLETADO**
Inclusión de 95/100 servidores virtuales en planes de backup Veeam	Equipo Infraestructura	T1 2026	**EN CURSO**
Ajuste y gestión de 209 servidores en planes ArcServe UDP (RPO 6h, 24h, semanal, mensual)	Equipo Infraestructura	T1 2026	**COMPLETADO**
Elaborar y aprobar procedimiento formal de respaldo y restauración (frecuencia, responsables, RTO/RPO)	Oficial de Seguridad	T1 - T2 2026	**PENDIENTE INFO**
Definir y ejecutar programa anual de pruebas de restauración sobre sistemas críticos	Oficial de Seguridad / Infraestructura	T2 - T3 2026	**PENDIENTE**

Fuente: Grupo TICS — Actividades Backup y Respaldo T1 2026 (24/03/2026)

2. Cumplimiento de Indicadores de Éxito (SLO): El proceso de estabilización presentó desafíos iniciales. Entre el 13 y el 21 de enero, el ratio de éxito de los respaldos (Successful Backup Ratio) experimentó una caída crítica, alcanzando niveles mínimos del 50%. Sin embargo, gracias a las labores de afinamiento, la plataforma recuperó su estabilidad, logrando mantener un indicador de éxito cercano al 100% durante la mayor parte de febrero y marzo.

3. Alineación de Tiempos de Recuperación (RTO y RPO) y Pruebas: En cumplimiento con las actividades del riesgo de alinear la herramienta con los requerimientos del BIA/BCP, se obtuvieron las siguientes métricas reales de recuperación:

- **RTO** (Objetivo de Tiempo de Recuperación): Se logró un RTO excelente en trabajos críticos, destacándose la recuperación exitosa del servicio CXCLOUD, el cual procesó 200 GB y fue restaurado en tan solo 15 minutos el 28 de marzo.

- **RPO** (Objetivo de Punto de Recuperación): Se implementaron políticas estrictas de RPO para los sistemas misionales, configurando respaldos incrementales con frecuencias de 6 horas Y 24 horas.

4. Protección contra Ransomware e Inmutabilidad: Para garantizar que los respaldos no sean alterados o secuestrados ante un posible ciberataque, se activó la protección multi-plataforma (Nutanix AHV y VMware) y se aprovechó la funcionalidad de repositorios inmutables de Veeam vXX. Esto asegura que, una vez ejecutado el backup, la información no pueda ser borrada ni cifrada por software malicioso durante el periodo de retención establecido.

5. Identificación de Cuellos de Botella y Optimización: Se identificó que el respaldo del servidor de archivos (Backup FILEUSER) es el trabajo más demandante, transfiriendo hasta 22 TB de datos y tomando un promedio de 1.50 horas por sesión. Durante marzo presentó advertencias (Warnings) que están siendo analizadas para prevenir fallos futuros.

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

El riesgo R21 aborda la brecha más crítica y estructural identificada en la gestión de seguridad del Ministerio: la ausencia de un inventario de activos de información completo, actualizado y alineado con los lineamientos del MSPI 2025. Sin esta base, resulta imposible desarrollar Análisis de Impacto al Negocio (BIA) confiables ni construir Planes de Continuidad del Negocio (BCP) efectivos. Esta brecha fue identificada desde las auditorías de 2025 y constituye un prerequisito para cualquier avance adicional en la madurez del SGSI.

Durante el primer trimestre de 2026, las actividades programadas para este riesgo corresponden al inicio del proceso de llenado de la matriz de activos con los delegados asignados por cada dependencia, en continuidad con la Circular 40028 expedida por la Secretaría General en septiembre de 2025. El cronograma estableció la segunda fase de capacitación de estos delegados durante la segunda y tercera semana de febrero, seguida del llenado inicial durante la tercera semana de febrero y la primera semana de marzo. La revisión primaria de la información enviada por las dependencias estaba programada para la segunda y tercera semana de marzo.

NOTA: El estado detallado de avance en el diligenciamiento de la matriz de activos, el número de dependencias con información entregada y el nivel de completitud alcanzado se encuentran dentro del plan de seguridad y privacidad de la información con mayor detalle

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

Durante el primer trimestre de 2026, la mitigación de este riesgo dio su paso más crucial al pasar de la fase de planeación a la fase de ejecución contractual y técnica:

1. Materialización y acta de Inicio del Proyecto CMS/CDA: El hito estratégico que garantiza la mitigación de este riesgo es el perfeccionamiento del **Contrato GGC-1755-2026**, suscrito con la Corporación Colombia Digital.

- **Inversión y Objeto:** El proyecto cuenta con un registro presupuestal de **$XX.X.X.000** (expedido el 30 de enero de 2026) y tiene como objeto directo fortalecer la solución integral de servicios de TI, ampliando las capacidades del Centro de Monitoreo Sectorial (CMS).
- **Ejecución:** Tras la aprobación de las pólizas de cumplimiento y responsabilidad civil durante el mes de febrero, se dio luz verde al plazo de ejecución de cinco (5) meses. Este proyecto dotará al Ministerio del anhelado nuevo Centro de Datos Alterno (CDA), así como de capacidades avanzadas de NOC y SOC y una arquitectura de seguridad en profundidad.

2. Despliegue Técnico y Operativo (Implementación DRP): A nivel técnico, los trabajos de implementación y configuración para la recuperación ante desastres ya iniciaron. Como evidencia de la operatividad en la infraestructura, los registros de auditoría de conexiones seguras (VPN SSL) del trimestre muestran sesiones activas de usuarios dedicados a esta labor, destacándose el acceso bajo el usuario *implementacion_drp2* durante el mes de enero.

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

El riesgo transversal de cultura de seguridad digital y gestión de identidades constituye uno de los retos más complejos de abordar, dado que su materialización depende del comportamiento humano y de la adopción de buenas prácticas por parte de todos los funcionarios y contratistas del Ministerio. Los seguimientos realizados en 2025 evidenciaron que únicamente el 78% de los colaboradores demostró estar alerta ante simulacros de phishing, lo que significa que el 22% restante continúa siendo un vector de riesgo potencial. Adicionalmente, persisten brechas en el uso de contraseñas robustas y en la adopción de mecanismos de autenticación multifactor (MFA).

Para 2026, el plan estableció tres líneas de acción: el diseño e implementación de un programa estructurado de sensibilización y capacitación con enfoque proactivo, la revisión y ajuste de las políticas de contraseñas evidenciado en las capacitaciones realizadas (las cuales se podrán encontrar con mayor detalle en el seguimiento del plan de seguridad y privacidad de la información primer trimestre) .

En segundo lugar, se configuró y activó de forma obligatoria el segundo factor de autenticación (2FA) en la plataforma Microsoft 365, de manera que la totalidad de los usuarios de la Entidad deben completar satisfactoriamente el proceso de verificación de identidad con múltiple factor para acceder a los recursos y servicios tecnológicos disponibles en dicho ecosistema. Esta medida de carácter técnico eliminó la posibilidad de acceso con credencial simple, reduciendo significativamente el riesgo de compromiso de cuentas institucionales ante ataques de phishing, robo de credenciales o accesos no autorizados.

En segundo lugar, y con el propósito de dar sustento normativo a dicho control, se estructuró la Política de Gestión de Identidades y Autenticación, instrumento que eleva la obligatoriedad del múltiple factor de autenticación al nivel normativo dentro del SGSI de la Entidad. Esta política establece que ninguna parte interesada podrá acceder a los sistemas institucionales sin haber completado el proceso de verificación de identidad con múltiple factor, define los mecanismos aceptados priorizando aplicaciones de autenticación para roles con acceso privilegiado o a información reservada y/o clasificada, y asigna al Grupo TICS y al Oficial de Seguridad de la Información la responsabilidad de su implementación y seguimiento mediante políticas de acceso condicional sin excepción.