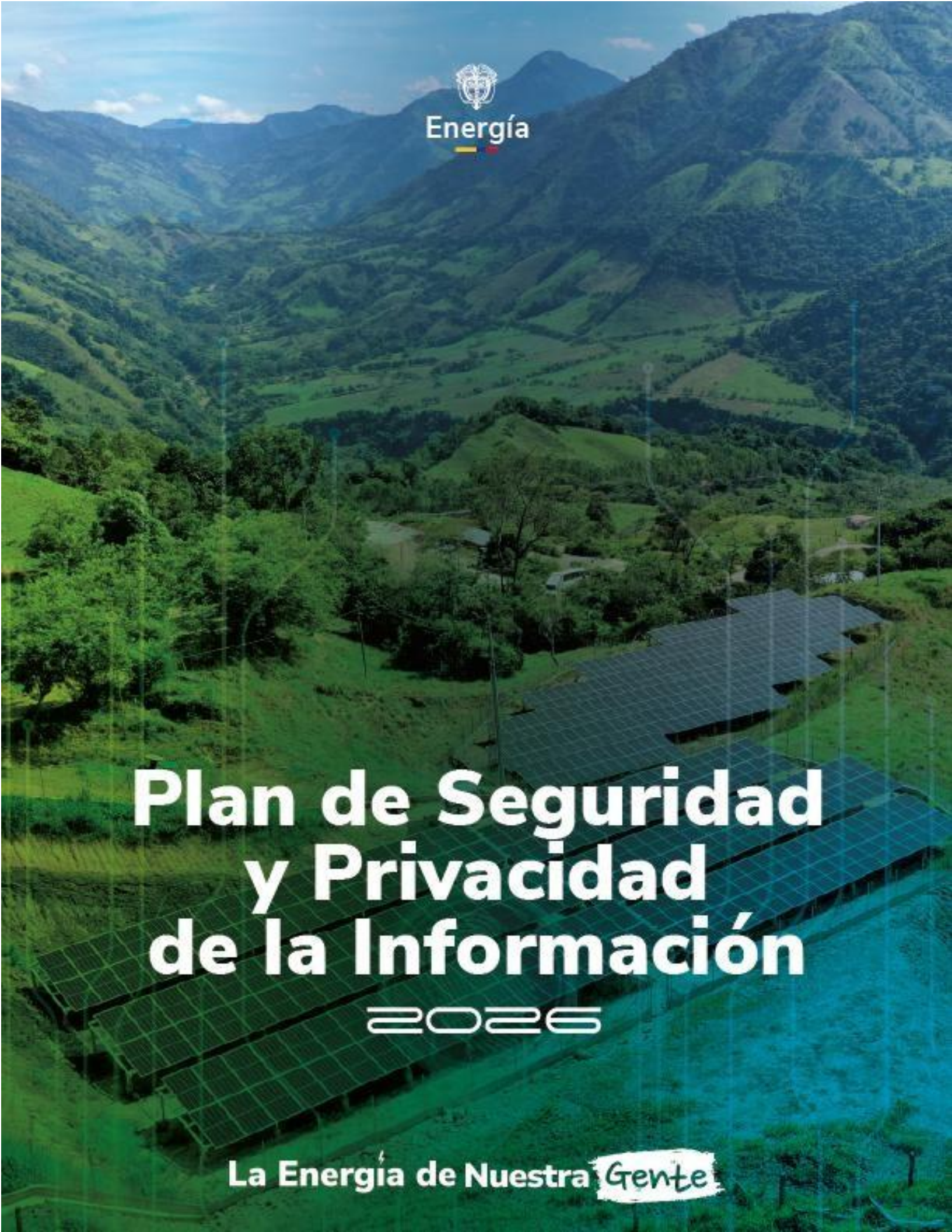

Plan de Seguridad y Privacidad de la Información

2026

La Energía de Nuestra Gente

Seguimiento Plan 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. DESCRIPCIÓN DEL INFORME

El presente informe corresponde al seguimiento del primer trimestre (enero-marzo de 2026) del Plan de Seguridad y Privacidad de la Información 2026 del Ministerio de Minas y Energía (MINENERGÍA), elaborado por el Grupo de Tecnologías de la Información y las Comunicaciones (GTIC) en cumplimiento del ciclo PHVA y de los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) versión 3.0.2 de MINTIC, así como de las normas ISO/IEC 27001:2022, ISO/IEC 22301:2019 e ISO/IEC 31000:2018.

El Plan de Seguridad y Privacidad de la Información 2026 definió tres pilares estratégicos: (1) Cumplimiento y mejora continua conforme a las brechas identificadas en 2025 y el ecosistema DevOps; (2) el cierre de brechas críticas, con especial énfasis en la actualización del inventario de activos de información, la alineación con el MSPI 2025 en infraestructura crítica cibernética, y la generación de BIA y BCP actualizados; y (3) el fortalecimiento de la resiliencia y continuidad operativa bajo el marco NIST CSF. Este seguimiento trimestral evalúa el avance en cada componente del plan operacional y del plan de aseguramiento, presentando los logros alcanzados, las actividades en curso y las pendientes de ejecutar para el segundo trimestre del año.

4. PLAN OPERACIONAL DE SEGURIDAD DE LA INFORMACIÓN

4.1 Gestión de activos de información

La gestión de activos de información constituye el cimiento del Sistema de Gestión de Seguridad de la Información (SGSI) del Ministerio de Minas y Energía y representa una de las brechas más significativas identificadas durante la vigencia 2025. En respuesta a esta realidad, el Plan de Seguridad y Privacidad de la Información 2026 incorporó un cronograma estructurado que, durante los meses de febrero y marzo, debía dar inicio a la segunda fase de capacitación de delegados por dependencia y al llenado inicial de la matriz de activos, herramienta que integra en un único instrumento los catálogos de licenciamiento, sistemas de información e infraestructura tecnológica, alineada con los lineamientos del MSPI.

La tabla siguiente refleja el estado de avance de las actividades programadas para el primer trimestre en el marco de la gestión de activos de información:

Tabla 1. Estado de actividades — Gestión de activos de información, 2026

Actividad	Responsable	Fecha Inicio	Fecha Fin	Estado T1 2026
Segunda fase capacitación sobre matriz de activos	Equipo Seguridad Información	2a sem Feb 2026	3a sem Feb 2026	**100%**
Llenado inicial de la matriz de activos	Responsables dependencias	3a sem Feb 2026	1a sem Mar 2026	**80%**
Segunda fase revisión primaria e información enviada por dependencias	Equipo Seguridad Información	2a sem Mar 2026	3a sem Mar 2026	**80%**
Ajustes y retroalimentación a dependencias faltantes	Equipo Seguridad Información	4a sem Mar 2026	1a sem Abr 2026	**100%**

La gestión de activos de información avanza de forma estructurada y con resultados concretos al cierre del primer trimestre. Del total de dependencias que conforman la estructura organizacional del Ministerio, únicamente diez (10) grupos no han remitido sus enlaces designados conforme al memorando de convocatoria, lo que representa un nivel de respuesta institucional significativamente alto frente al compromiso formalizado mediante la Circular 40028 de 2025.

Con el propósito de gestionar el proceso de manera ordenada y garantizar un seguimiento efectivo, las dependencias fueron organizadas en cuatro (4) grupos conforme a la cronología de envío de sus enlaces, permitiendo al equipo de seguridad de la información llevar un control diferenciado por etapa:

El Grupo 01 y el Grupo 02 han completado el proceso de diligenciamiento de sus matrices de activos de información y recibieron la retroalimentación correspondiente por parte del equipo del GTIC, dando por finalizada la gestión en estas dependencias.

El Grupo 03 se encuentra actualmente en la fase de diligenciamiento de la matriz, a la espera de finalizar el registro para proceder con la revisión, unificación de información y la respectiva retroalimentación.

El Grupo 04, conformado por las diez dependencias pendientes de reporte, participará en la última sesión de capacitación sobre gestión de activos de información, programada para el día 13 de abril de 2026, espacio en el que se espera dar cierre definitivo a esta fase del proceso.

En paralelo, el equipo de seguridad de la información viene adelantando, en coordinación con el equipo de PMO del Grupo TICS, el desarrollo del Procedimiento de Gestión de Activos de Información, con el objetivo de formalizar institucionalmente la metodología aplicada y garantizar su sostenibilidad en el tiempo.

La totalidad de las evidencias del proceso) incluyendo actas de asistencia a capacitaciones, registros de mesas de trabajo y retroalimentaciones de las 49 dependencias que ya han cumplido con su entrega) se encuentran debidamente archivadas en la carpeta interna del SGSI y en el sitio de SharePoint correspondiente al módulo de Activos de Información.

4.2 Gestión de BIA y BCP

En el marco de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y la estructuración de la arquitectura de continuidad del negocio del Ministerio de Minas y Energía, durante el primer trimestre de 2026 se adelantaron actividades concretas y estructuradas orientadas al desarrollo del Análisis de Impacto al Negocio (BIA) institucional. Este ejercicio constituye un insumo crítico e indispensable para la formulación de las estrategias de continuidad del negocio (BCP) y el Plan de Recuperación ante Desastres (DRP), herramientas que a su vez alimentan la definición de controles precisos dentro del SGSI y la correcta gestión del Riesgo R23.

Definición metodológica. Como punto de partida del proceso, se elaboró la primera versión de la Guía BIA institucional del MINENERGÍA, documento que establece la metodología aplicable para la identificación de procesos críticos, la evaluación de impactos derivados de su interrupción, la definición de los tiempos de recuperación requeridos (MTPD, RTO y RPO) y la clasificación de criticidad por proceso. Esta guía se encuentra completada y se encuentra pendiente de validación formal por parte de la Oficina de Planeación, paso necesario para su adopción institucional definitiva.

Levantamiento de información: Se adelantó el levantamiento de información con las dependencias del Ministerio mediante acompañamiento técnico directo y seguimiento al diligenciamiento de los formatos BIA. Al cierre del primer trimestre, el avance cuantitativo del levantamiento es el siguiente: de un total de 19 procesos identificados, se han levantado y analizado 8 procesos, equivalentes al 42% de avance, quedando pendientes 11 procesos para completar la cobertura total. Los procesos abordados a la fecha incluyen: Gestión Administrativa, Gestión Contractual, Dirección de Minería Empresarial, Asuntos Nucleares, Gestión de Recursos Físicos, entre otros.

Matriz Maestra BIA. En paralelo al levantamiento de información, se construyó la Matriz Maestra BIA del Ministerio, instrumento que integra de manera consolidada los procesos y funciones críticas identificados, los sistemas y activos de información asociados, los impactos operativos, legales y reputacionales derivados de interrupciones, los tiempos de recuperación definidos y las dependencias entre procesos. Esta matriz se encuentra parcialmente consolidada y en actualización continua conforme avanza el levantamiento con las dependencias restantes.

Análisis de tiempos de recuperación. Con base en la información recopilada, se generó un consolidado preliminar de tiempos de recuperación que incluye la parametrización del MTPD (Maximum Tolerable Period of Disruption), RTO (Recovery Time Objective) y RPO (Recovery Point Objective), la clasificación de procesos por niveles de criticidad (Tier 1, 2 y 3) y las estrategias de continuidad preliminares asociadas a cada nivel. Este análisis se encuentra en estado preliminar, sujeto a ajuste una vez se complete el levantamiento del 58% restante y se validen los tiempos con los dueños de proceso.

Identificación de riesgos y articulación con arquitectura. El ejercicio BIA permitió identificar riesgos asociados a sistemas críticos con baja tolerancia a la interrupción, dependencias externas con impacto en la operación del Ministerio, y escenarios de impacto legal y operativo. Adicionalmente, el proceso se encuentra articulado con el Plan MAE (Modelo de Arquitectura Empresarial), la arquitectura de seguridad institucional y el diseño de continuidad del negocio, garantizando coherencia entre los distintos instrumentos de gestión tecnológica del GTIC.

Dificultades identificadas. Durante el primer trimestre se identificaron las siguientes dificultades que requieren atención para garantizar el cierre oportuno del BIA: retrasos en la entrega de información por parte de algunas dependencias, diferencias en los niveles de madurez y apropiación del proceso entre áreas, necesidad de mayor acompañamiento técnico en algunas dependencias, y validación pendiente de los tiempos críticos con los respectivos dueños de proceso.

4.3 Tratamiento de riesgos de seguridad de la información

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 2. Acciones de seguimiento y cumplimento para cada uno de los riesgos mapeados para el primer trimestre

Tabla 2

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.

Para más información del desarrollo de cada uno de los riegos y su debida implementación con los controles respectivos, se debe revisar el seguimiento primer trimestre al plan de tratamiento de riesgos de seguridad de la información 2026.

4.4 Gestión de políticas y procedimientos

Durante el primer trimestre de 2026, el Ministerio de Minas y Energía avanzó de forma significativa en la formalización y actualización de los instrumentos normativos que soportan el Sistema de Gestión de Seguridad de la Información (SGSI), logrando la integración de tres documentos al Sistema Integrado de Gestión (SIG) de la Entidad a través de la Oficina de Planeación y Gestión Internacional.

Instrumentos formalizados e integrados al SIG:

Los siguientes documentos fueron elaborados, revisados, aprobados e integrados formalmente al sistema de gestión de calidad de la Entidad durante el primer trimestre de 2026:

1. **Procedimiento para el monitoreo y gestión de incidentes de seguridad de la información (T-GT-P-23, V-1, 13-04-2026):** Establece las directrices, actividades y responsabilidades para la gestión integral de incidentes de seguridad de la información, abarcando desde la detección temprana y el triage hasta la contención, remediación, documentación y análisis post-incidente. El procedimiento se soporta en las capacidades de monitoreo continuo 24/7 del SOC y contempla la articulación con el CSIRT sectorial y el COLCERT cuando aplique. Define una clasificación de incidentes por nivel de impacto (Alta, Media, Baja, Desconocida) frente a las dimensiones de confidencialidad, integridad y disponibilidad, y establece 19 actividades formales en su ciclo de vida, con responsabilidades asignadas al SOC, el Grupo TIC, el Oficial de Seguridad de la Información (CISO) y el equipo de operaciones.

2. **Procedimiento de gestión de vulnerabilidades :** Establece el proceso sistemático para identificar, registrar, clasificar, priorizar, tratar, verificar y hacer seguimiento a las

vulnerabilidades técnicas presentes en los activos de información institucionales, en cumplimiento del control 8.8 de la norma ISO/IEC 27001:2022. El procedimiento define tres ciclos cuatrimestrales de análisis al año (enero-abril, mayo-agosto, septiembre-diciembre), con plazos de subsanación diferenciados según la severidad CVSS 3.1: crítico (≤10 días), alto (≤30 días), medio (≤60 días) y bajo (≤90 días). La gestión y trazabilidad de los hallazgos se realiza a través de la herramienta ITSM institucional.

3. **Guía de cifrado para transferencia de archivos internos y externos (T-GT-G-01, V-2, 13-04-2026):** Establece el proceso estandarizado y seguro para el cifrado y la transferencia de archivos clasificados como confidenciales o sensibles, tanto en el ámbito interno como externo. Define los algoritmos de cifrado recomendados (AES-256, RSA, XChaCha20-Poly1305), las herramientas autorizadas (7-Zip, WinRAR, Kaspersky, BitLocker), los canales de transferencia seguros (correo electrónico con S/MIME o TLS, SFTP/FTPS y SharePoint) y los criterios de manejo según el tamaño del archivo. Adicionalmente, establece lineamientos para la gestión segura de contraseñas de cifrado y el registro centralizado de cada transferencia.

Instrumento en proceso de formalización:

La Política de Gestión de Identidades y Autenticación, que establece la autenticación multifactor (MFA) como control obligatorio para el acceso a todos los recursos tecnológicos de la Entidad, se encuentra elaborada y en proceso de formalización ante la Oficina de Planeación. Esta política define los mecanismos de múltiple factor aceptados, las responsabilidades del Grupo TICS y del Oficial de Seguridad de la Información en su implementación mediante políticas de acceso condicional, y las condiciones de excepción y revisión periódica. Su formalización e integración al SIG se proyecta para el segundo trimestre de 2026.

Instrumentos proyectados para el segundo trimestre de 2026:

En el marco de la gestión de activos de información, durante el segundo trimestre de 2026 se tiene previsto avanzar en la formalización de los siguientes instrumentos:

- **Procedimiento de Gestión de Activos de Información,** que establecerá el ciclo de vida completo para la identificación, registro, clasificación, mantenimiento y baja de activos de información institucionales en el marco del SGSI.
- **Matriz de Activos de Información,** instrumento que permitirá consolidar el inventario oficial de activos de información de la Entidad, incluyendo su valoración frente a las dimensiones de confidencialidad, integridad y disponibilidad, así como la asignación de custodios y propietarios responsables.

Ambos instrumentos constituyen un insumo fundamental para el fortalecimiento de los controles del SGSI y la gestión de riesgos de seguridad de la información de la Entidad.

4.5 Gestión de recursos de seguridad

Durante el primer trimestre de 2026, la gestión de recursos de seguridad se ha enfocado en la consolidación de proyectos estratégicos y la optimización de las plataformas de ciberseguridad existentes:

1. Puesta en marcha de la Fase 2 del Centro de Monitoreo Sectorial (CMS): Como hito principal para la resiliencia del Ministerio y la protección de la infraestructura crítica, se dio inicio a la Fase 2 del Centro de Monitoreo Sectorial mediante el Contrato GGC-1755-2026, suscrito en febrero de 2026. Este proyecto de gran envergadura permite la puesta en marcha oficial del **Centro de Datos Alterno (CDA)**, así como el despliegue de las capacidades operativas del **SOC (Security Operations Center)** y el **CSIRT** sectorial. Esto mitigará directamente los riesgos históricos asociados a la falta de un DRP (Plan de Recuperación ante Desastres) consolidado.

2. Planeación y renovación de herramientas avanzadas de seguridad: En cumplimiento de la estrategia de mantener soluciones tecnológicas de vanguardia para el monitoreo continuo y la gestión de vulnerabilidades, se está contemplando la **renovación de las licencias de Darktrace** (para la detección y respuesta de red basada en IA) y la **renovación de Tenable** (para la gestión integral de vulnerabilidades) y el diseño del proyecto de inversión hacia un análisis de ethical hacking externo con ingeniería social . Estas renovaciones se alinean con la actividad planificada de establecer las necesidades de presupuesto en seguridad proyectada para el segundo trimestre.

3. Optimización y licenciamiento de la infraestructura de seguridad actual: Paralelo a las nuevas inversiones, se garantizó el funcionamiento y actualización de las plataformas existentes que protegen el perímetro y los endpoints:

- **Seguridad Perimetral :** Los equipos FortiGate XXXX en Alta Disponibilidad (HA) operan de manera estable, con licenciamiento integral vigente hasta el XX de diciembre de 2026. Durante este trimestre se realizó la actualización del firmware a la versión estable vX.X.XX y se depuraron las políticas del WAF, optimizando el consumo de CPU (menor al 10%) y memoria (menor al 50%).
- **Protección de Endpoints :** Se mantiene el control sobre el licenciamiento adquirido de 1.200 unidades. Al cierre del trimestre, se registraron aproximadamente 475 licencias en uso. Se están adelantando labores de depuración del Directorio Activo para instalar el agente de seguridad en los equipos faltantes y aprovechar al máximo el recurso adquirido.
- **Sistemas de Respaldo :** Se implementó la versión XX de XXXX Backup & Replication con un licenciamiento adquirido para 100 nodos. Al mes de marzo, se están respaldando exitosamente 95 servidores virtuales. Se ha identificado la necesidad de adquirir el licenciamiento completo para la totalidad de los servidores físicos y virtuales de la entidad para ampliar la cobertura de protección y minimizar riesgos

Nota : se deja en “XX” información pertinente a equipos confidenciales, si se requiere más información se debe solicitar al oficial de seguridad de la información de la entidad.

4.6 Gestión de indicadores de seguridad de la información

Durante el primer trimestre de 2026, el avance en la gestión de indicadores ha cumplido con el cronograma establecido en el plan estratégico:

- Definición de indicadores clave (Feb - Mar): Se establecieron las métricas base operativas y de seguridad.
- Recolección inicial de datos (Mar - Abr): Se consolidó la línea base del Q1 a partir de las plataformas de seguridad y monitoreo.

A continuación, se presenta la consolidación robusta de los indicadores de gestión y desempeño de seguridad recolectados durante este trimestre:

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.

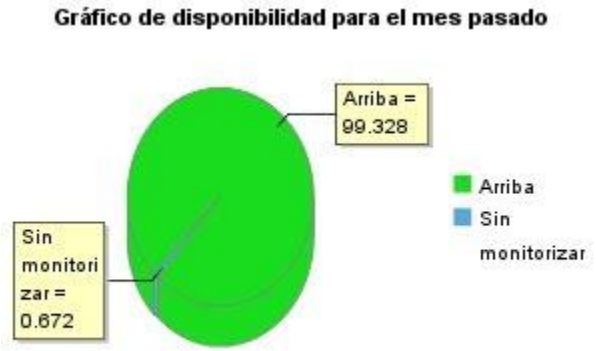

Imagen [1]. Grafico de disponibilidad firewall para el primer trimestre 2026

Estadísticas de disponibilidad	
Opciones	Tiempo de actividad (%)
Hoy	100.0%
Ayer	100.0%
Ultimos 7 dias	100.0%
Ultimos 30 dias	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 [2]. Disponibilidad firewall para el primer trimestre 2026

- **Web Application Firewall (WAF):** El servicio operó con una disponibilidad del 99.3% en enero, alcanzó el 100% en febrero y presentó una leve disminución al 96.9% en marzo.

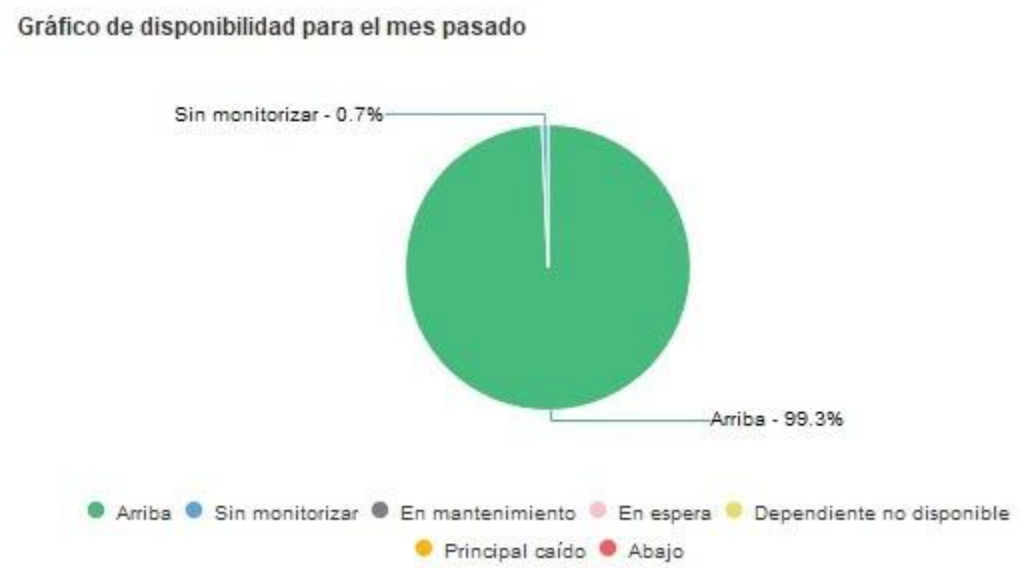

Imagen [3]. Disponibilidad WAF para el mes de Enero 2026

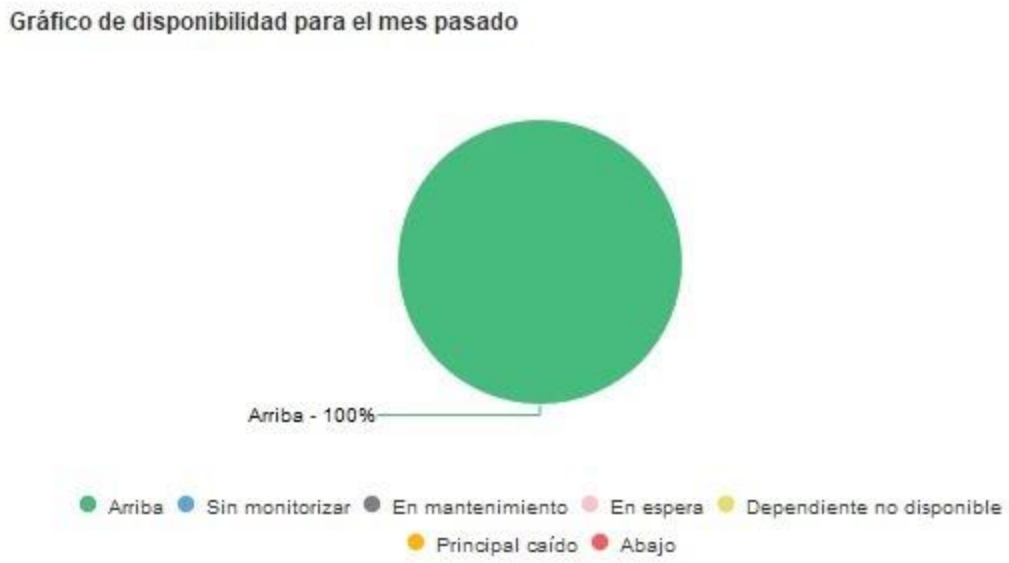

Imagen [4]. Disponibilidad WAF para el mes de Febrero 2026

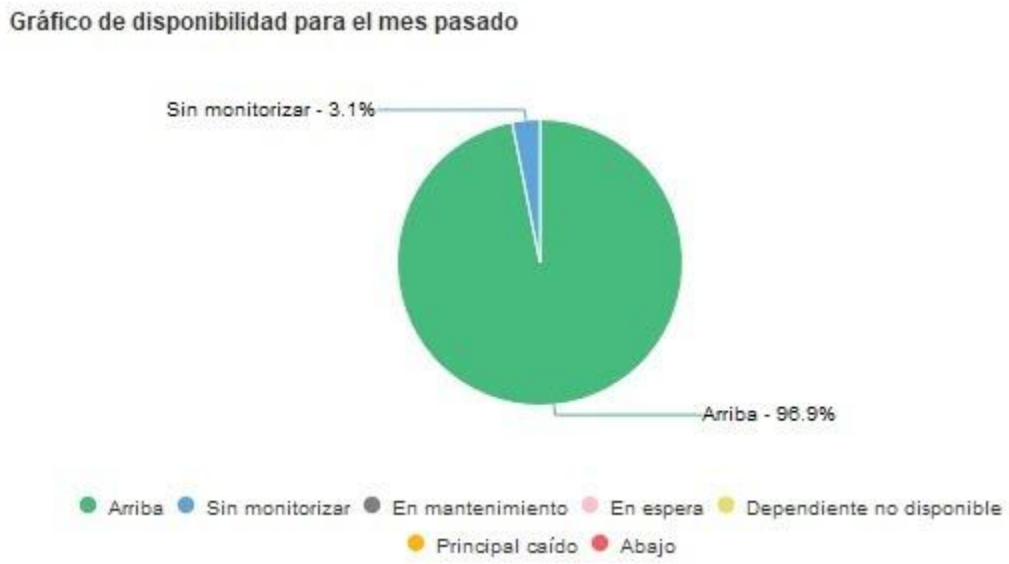

Imagen [5]. Disponibilidad WAF para el mes de Marzo 2026

- **Enlaces de Conectividad (Media Commerce):** La disponibilidad promedio general de los enlaces de datos e internet se mantuvo en el 100%, 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).

A continuación se muestra una imagen de los informes presentados por el proveedor en términos de disponibilidad del servicio de conectividad.

	ENLACE	AVAILABILITY
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Bkp Item 6	100,00 %
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Item 5	100,00 %
	CAPITAL INVESTMENTS Diag 5A No 3-10 Sur Soacha Item 7	99,72 %
14/03/2026		
	CAPITAL INVESTMENTS BK DIAGONAL 5A # 3-10 SUR-SOACHA C/MARCA ITEM 10	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Bogota Item 2	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Centro Administrativo Nacional Bogota Item 3	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Centro Administrativo Nacional Bogota Item 4	100,00 %
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Bkp Item 6	100,00 %
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Item 5	100,00 %
	CAPITAL INVESTMENTS Diag 5A No 3-10 Sur Soacha Item 7	100,00 %
15/03/2026		
	CAPITAL INVESTMENTS BK DIAGONAL 5A # 3-10 SUR-SOACHA C/MARCA ITEM 10	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Bogota Item 2	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Centro Administrativo Nacional Bogota Item 3	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Centro Administrativo Nacional Bogota Item 4	100,00 %
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Bkp Item 6	100,00 %
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Item 5	100,00 %
	CAPITAL INVESTMENTS Diag 5A No 3-10 Sur Soacha Item 7	100,00 %
16/03/2026		
	CAPITAL INVESTMENTS BK DIAGONAL 5A # 3-10 SUR-SOACHA C/MARCA ITEM 10	88,73 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Bogota Item 2	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Centro Administrativo Nacional Bogota Item 3	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Centro Administrativo Nacional Bogota Item 4	100,00 %
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Bkp Item 6	100,00 %
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Item 5	100,00 %
	CAPITAL INVESTMENTS Diag 5A No 3-10 Sur Soacha Item 7	99,86 %
17/03/2026		
	CAPITAL INVESTMENTS BK DIAGONAL 5A # 3-10 SUR-SOACHA C/MARCA ITEM 10	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Bogota Item 2	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Centro Administrativo Nacional Bogota Item 3	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Centro Administrativo Nacional Bogota Item 4	100,00 %
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Bkp Item 6	100,00 %
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Item 5	100,00 %
	CAPITAL INVESTMENTS Diag 5A No 3-10 Sur Soacha Item 7	100,00 %
18/03/2026		
	CAPITAL INVESTMENTS BK DIAGONAL 5A # 3-10 SUR-SOACHA C/MARCA ITEM 10	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Bogota Item 2	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Centro Administrativo Nacional Bogota Item 3	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Centro Administrativo Nacional Bogota Item 4	100,00 %
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Bkp Item 6	100,00 %
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Item 5	100,00 %
	CAPITAL INVESTMENTS Diag 5A No 3-10 Sur Soacha Item 7	98,48 %
19/03/2026		
	CAPITAL INVESTMENTS BK DIAGONAL 5A # 3-10 SUR-SOACHA C/MARCA ITEM 10	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Bogota Item 2	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Centro Administrativo Nacional Bogota Item 3	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Centro Administrativo Nacional Bogota Item 4	100,00 %
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Bkp Item 6	100,00 %
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Item 5	100,00 %
	CAPITAL INVESTMENTS Diag 5A No 3-10 Sur Soacha Item 7	100,00 %
20/03/2026		
	CAPITAL INVESTMENTS BK DIAGONAL 5A # 3-10 SUR-SOACHA C/MARCA ITEM 10	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Bogota Item 2	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Centro Administrativo Nacional Bogota Item 3	100,00 %
	CAPITAL INVESTMENTS Cll 43 # 57-31 Centro Administrativo Nacional Bogota Item 4	100,00 %
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Bkp Item 6	100,00 %
	CAPITAL INVESTMENTS Cra 50 # 26-20 Bogota Item 5	100,00 %

Imagen [6]. Disponibilidad informe proveedor para primer trimestre 2026

2. Indicadores de Protección de Endpoints :

- **Cobertura de licenciamiento**: De un total de 1.200 licencias adquiridas, se cerró el mes de febrero con 475 licencias en uso. Este indicador subraya la necesidad de acelerar el despliegue del agente en los equipos restantes.

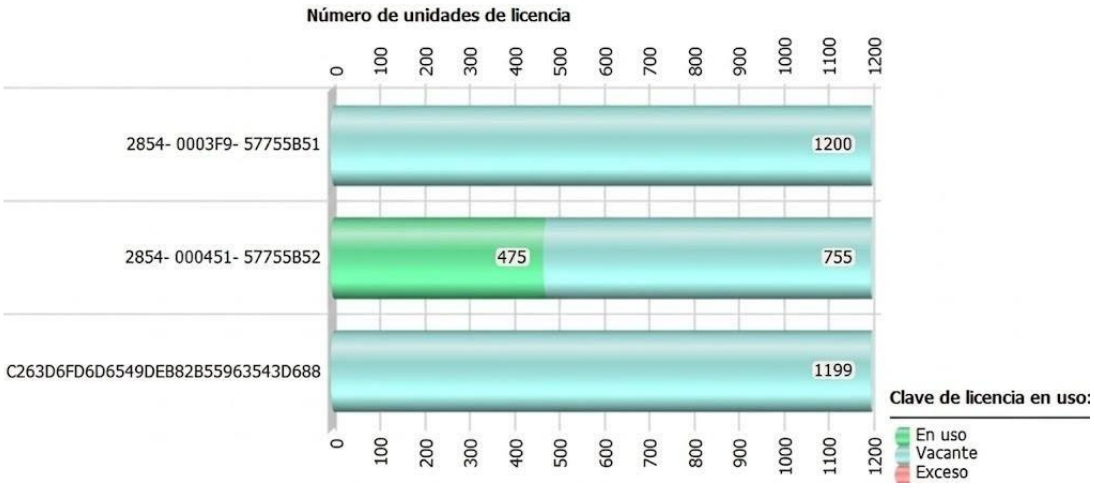

Imagen [7]. Licenciamiento de endpoints para la infraestructura de TI del Ministerio.

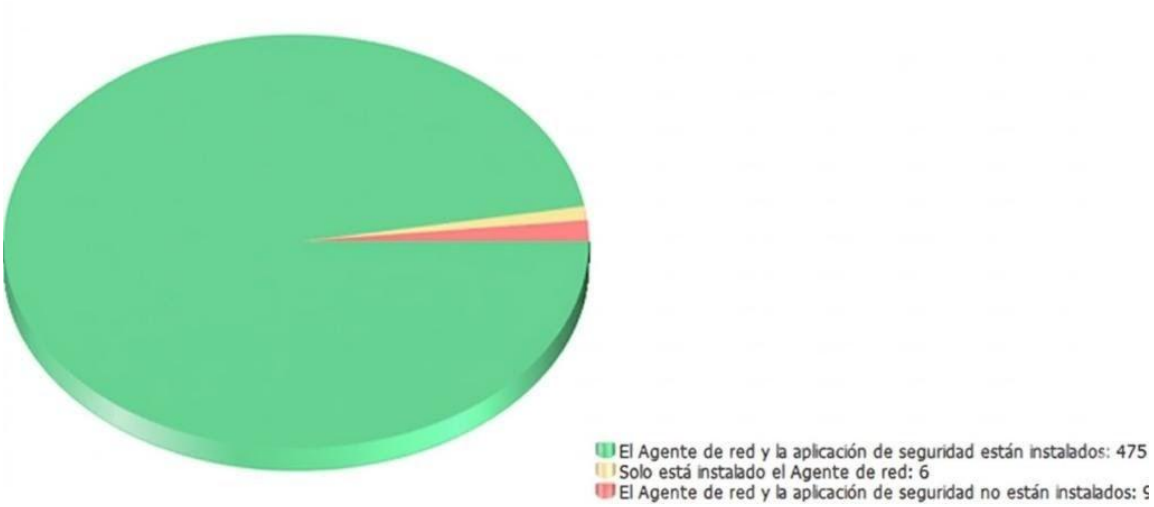

Imagen [8]. Licenciamiento de endpoints para la infraestructura de TI del Ministerio.

- **Gestión de Vulnerabilidades de Software:** Se evidenció una disminución positiva en las vulnerabilidades críticas detectadas en los equipos. En enero se reportaron 197 dispositivos con vulnerabilidades de gravedad crítica, cifra que disminuyó a 182 en el mes de febrero. Las vulnerabilidades de gravedad alta también bajaron de 68 a 61.

Imagen [9]. 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 febrero se eliminaron 84 registros de amenazas de los dispositivos.

Imagen [10]. Bloqueo de amenazas enero-febrero 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.

3. Indicadores de Respaldo y Recuperación (Veeam Backup):

- **Ratio de Éxito de Backups (SLO):** El indicador de respaldos exitosos sufrió una caída crítica (al 50%) entre el 13 y el 21 de enero, pero se logró estabilizar logrando un éxito cercano al 100% durante febrero y la mayor parte de marzo.
- **Objetivos de Tiempo de Recuperación (RTO):** Se logró medir un RTO excelente para trabajos críticos (como CXCLOUD), logrando la recuperación de volúmenes en aproximadamente 15 minutos.

4. Indicadores de Cumplimiento Estratégico:

- Avance Análisis de Impacto al Negocio (BIA): El levantamiento de información para los procesos críticos cerró el trimestre con un avance del 42%, logrando mapear 8 de los 19 procesos totales identificados.

4.7 Afinamiento de la ciberseguridad

El Informe de Afinamiento del Firewall correspondiente al período enero-marzo de 2026 evidencia que el equipo maestro del Ministerio opera con parámetros óptimos de desempeño. El consumo de CPU se mantiene por debajo del 10%, el uso de memoria es inferior al 50% (tendencia sostenida respecto al período anterior) y las sesiones concurrentes son inferiores a 50.000, registrando una reducción promedio de 10.000 sesiones respecto al trimestre anterior. El equipo opera con XX núcleos de procesador en funcionamiento normal y el clúster HA Activo-Pasivo se encuentra sincronizado y operativo.

Se destaca que durante el trimestre se registró un apagado inesperado del datacenter que motivó el reinicio del equipo; sin embargo, gracias a la configuración HA y a la sincronización del clúster, la continuidad del servicio no fue afectada. El clúster está compuesto por el nodo maestro XXXXX_FW_X (serial XXXXXXXXX, prioridad XX) y el nodo esclavo XXXXX_FW_XX (serial XXXXXXXXX, prioridad XXX), ambos en estado sincronizado. Los logs se almacenan en tiempo real en el XXXX (IP XXX.XXX..X..X), garantizando la trazabilidad de eventos para auditoría y generación de reportes. El agente FSSO se encuentra activo contra el servidor XXX.XX.XXX permitiendo la identificación de usuarios para la gestión de permisos de navegación.

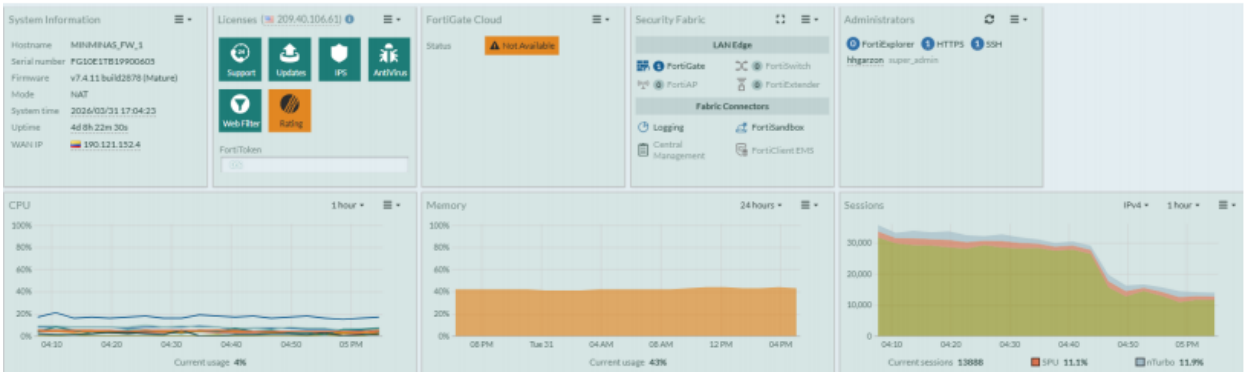

Imagen [11]. Consumo de memoria y CPU primer trimestre 2026

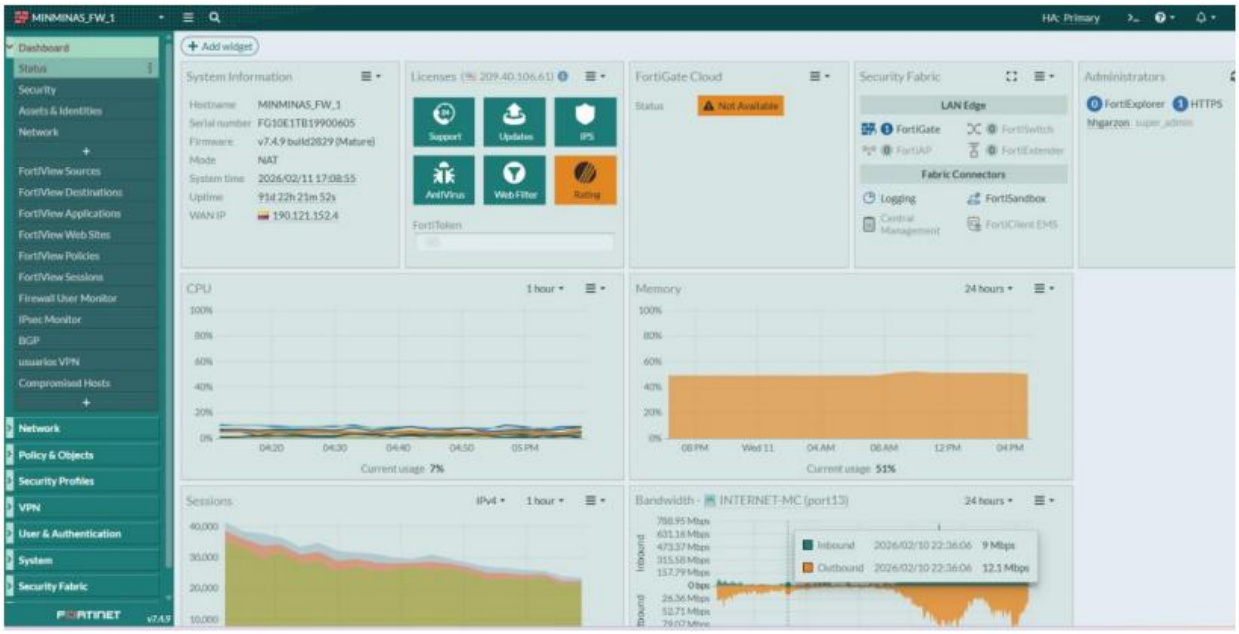

Imagen [12]. Bloqueo de amenazas primer trimestre 2026

Imagen [13]. Estado HA del cluster primer trimestre 2026

Tabla 3. Actividades de afinamiento realizadas – XXXXXXX 2026

Actividad de Afinamiento	Estado	Período
Depuración de 7 políticas WAF obsoletas (quedan 125 activas)	COMPLETADO	T1 2026
Desactivación de modo monitor en 3 políticas WAF	COMPLETADO	T1 2026
Desactivación de protocolo HTTP en publicaciones de portales institucionales	COMPLETADO	T1 2026
Asignación de perfil de protección web personalizado a 7 aplicaciones con perfil predeterminado	COMPLETADO	T1 2026
Bloqueo de IPs maliciosas con IoC de Colcert, Csirt y SOC de la entidad	COMPLETADO	T1 2026
Actualización de XXXXX HA de versionamiento	COMPLETADO	Enero 2026
Actualización del analizador perimetral	COMPLETADO	Febrero 2026

Fuente: Informe de Afinamiento– Enero-Marzo 2026

Las actividades de afinamiento realizadas durante el trimestre evidencian un enfoque proactivo en la reducción de la superficie de ataque y en la optimización de la configuración de seguridad. La depuración de 7 políticas WAF obsoletas, la asignación de perfiles de protección web personalizados en sustitución de perfiles predeterminados, y la desactivación del protocolo HTTP en las publicaciones de portales institucionales son medidas que reducen directamente la exposición a amenazas externas. El bloqueo de IPs maliciosas con base en indicadores de compromiso (IoC) provenientes de Colcert, Csirt y el SOC de la entidad refuerza la detección y respuesta ante amenazas activas dirigidas al Ministerio.

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

4.8 Plan de auditorias

De acuerdo con el Plan de Seguridad y Privacidad de la Información 2026, las actividades relacionadas con las auditorías de seguridad están programadas para el tercer trimestre del año (junio-octubre de 2026), incluyendo el establecimiento del perfil del equipo auditor, la definición del grupo auditor, la ejecución de la auditoría y la presentación del informe correspondiente. Por lo tanto, durante el primer trimestre no se reportan actividades formales de auditoría; el inicio del proceso se prevé para la primera semana de junio de 2026, con participación de la Oficina de Control Interno como responsable principal

4.8 Gestión de vulnerabilidades

Durante el primer trimestre del año 2026, y conforme a las actividades establecidas en el Plan de Seguridad y Privacidad de la Información, se dio inicio a la implementación del repositorio institucional de seguimiento a vulnerabilidade. Este repositorio tiene como finalidad centralizar, documentar y dar trazabilidad a todas las actividades de detección, análisis, tratamiento y cierre de vulnerabilidades técnicas, garantizando así un control sistemático y continuo sobre las debilidades que puedan afectar la infraestructura tecnológica y los sistemas de información críticos del Ministerio de Minas y Energía.

Como parte del proceso, a partir del 10 de marzo de 2026, se definieron los sistemas de información priorizados para el análisis de vulnerabilidades, conforme a criterios de criticidad técnica, funcional y operativa establecidos por el Grupo de Infraestructura Tecnológica. Esta priorización se basa en el nivel de exposición de los sistemas, su valor estratégico para la entidad, y su impacto potencial frente a incidentes de seguridad. Con este enfoque, se busca optimizar los recursos y asegurar la protección de los activos más sensibles, alineando esta actividad con los principios de gestión basada en riesgos y con los lineamientos de la norma ISO/IEC 27002:2022 en su sección de gestión de vulnerabilidades técnicas.

La siguiente tabla presenta el cronograma de ejecución para el análisis de vulnerabilidades de los sistemas priorizados, incluyendo fechas estimadas, responsables técnicos, y mecanismos de verificación y cierre. Esta actividad es complementaria a los controles definidos en el plan de tratamiento de riesgos y se articula con los demás componentes del Sistema de Gestión de Seguridad de la Información (SGSI), fortaleciendo así la postura institucional en ciberseguridad y aseguramiento digital.

Tabla 6

Cronograma de vulnerabilidades

APLICACIÓN	FECHA
IFX_repositoriobi	SEMANA 1
NORMATIVAMME	SEMANA 1
IFX_PORTAL_MME_HTTPS	SEMANA 1
Aula Virtual	SEMANA 1
Biblioteca	SEMANA 1
Suime 3 Fondo BEcas	SEMANA 1
IFX_WEBGLP	SEMANA 2
IFX_SISEG	SEMANA 2
GITLAB	SEMANA 2
IFX_SIPRIVADO	SEMANA 2
IFX_MESADEAYUDA	SEMANA 2
IFX_SERVICIOS	SEMANA 2
Directorio Activo	SEMANA 2
IFX_REPORTES_SISEG ENERGIA	SEMANA 3
IFX_GEOVISOR	SEMANA 3
IFX_EITI_COLOMBIA 179.1.211.170 172.17.10.125	SEMANA 3
SARA_	SEMANA 3
sith.minminas.gov.co_ifx	SEMANA 3
siveeic_http	SEMANA 3
siveic_https	SEMANA 3
siveic_3020	SEMANA 3
siveic_3010	SEMANA 3
Servidores Virtuales	SEMANA3

GRC	SEMANA 4
Portal_autogestion_accesos	SEMANA 4
Argopruebas	SEMANA 4
VIP_ARGOP	SEMANA 4
ARGO_CALIDAD	SEMANA 4
ARGO-DEV	SEMANA 4
argo_QA	SEMANA 4
SGP	SEMANA 4
Servidores Fisicos	SEMANA 4
SIGAME	SEMANA 5
Sara_TH	SEMANA 5
VIP_sisegdee	SEMANA 5
SISEGDH	SEMANA 5
NEON PRODUCCION	SEMANA 5
NEON_PRUEBAS	SEMANA 5
AVANZAME	SEMANA 5
AVANZAME_PROD	SEMANA 5
VIP_declaragas	SEMANA 6
VIP_geoserver	SEMANA 6
cargamap.minenergia	SEMANA 6
SARA_HTTPS	SEMANA 6
SERV_CREDITOBID	SEMANA 6
XROAD-QA	SEMANA 6
Mesa ayuda admin	SEMANA 6
VIP_ARGISENTERPRISE	SEMANA 7
VIP-ARGO-QA	SEMANA 7
sara 8480	SEMANA 7
GEONETWORK_PROD	SEMANA 7

SISEG-DH-PRUEBAS	SEMANA 7
JBPM-QA	SEMANA 7
TRANSPARENCIA_PROD	SEMANA 7
Energia evoluciona	SEMANA 7
SITH_PRUEBAS	SEMANA 8
CULTURA ENCUESTAS	SEMANA 8
WEBGLP 8081	SEMANA 8
WEBGLP 8082	SEMANA 8
OAAS VISOR CONFLICTOS	SEMANA 8
ASISTENTE VIRTUAL	SEMANA 8
ODKCENTRAL	SEMANA 8
TRAMITES	SEMANA 8
PGRD	SEMANA 8
pigccme.minenergia.gov.co	SEMANA 8
Intégrame	SEMANA 8
P8	Se validará al final que se hace con estas aplicaciones
Correspondencia SEERV MMECE Histórico	Se validará al final que se hace con estas aplicaciones
SIGME	Dejar de publicar

Para mayor detalle sobre el cumplimiento y los resultados obtenidos en los análisis de vulnerabilidades realizados durante el primer trimestre de 2026, se recomienda consultar directamente con el Oficial de Seguridad de la Información, quien centraliza y gestiona los informes técnicos correspondientes. Durante este periodo, se ejecutaron las actividades de escaneo y evaluación inicial de vulnerabilidades sobre los sistemas priorizados, conforme al cronograma establecido.

Se prevé que, en el segundo trimestre, se realicen las acciones de remediación necesarias con base en las recomendaciones emitidas en los informes, y posteriormente se llevará a cabo un retest técnico, con el objetivo de verificar y evidenciar de manera objetiva el cierre efectivo de las brechas identificadas. Este proceso permitirá validar la eficacia de las medidas aplicadas y alimentar el ciclo de mejora continua del SGSI.

4.10 Capacitación y sensibilización

Durante el primer trimestre de 2026, el Grupo de Tecnologías de la Información y las Comunicaciones (TICS), en coordinación con el área de Comunicaciones, aprobó y socializó el Cronograma de Capacitación en Seguridad de la Información para la vigencia 2026, instrumento que contempla un total de 14 sesiones de formación distribuidas a lo largo del año, orientadas a fortalecer la cultura de seguridad digital y los hábitos de higiene digital entre los funcionarios y contratistas del Ministerio de Minas y Energía.

Las sesiones programadas abordan temáticas alineadas con los controles del SGSI y los riesgos identificados en el entorno institucional, con el propósito de generar conciencia y apropiación de las buenas prácticas en el manejo de la información, el uso responsable de los recursos tecnológicos y la prevención de incidentes de seguridad.

En el marco de la ejecución de dicho cronograma, el 18 de marzo de 2026 se llevó a cabo la primera sesión de capacitación del año, centrada en las políticas de seguridad de la información vigentes en el Ministerio de Minas y Energía. La sesión tuvo una duración de 1 hora y 30 minutos y contó con la participación de 66 asistentes, registrados a través del formulario de asistencia habilitado para el evento. Esta capacitación permitió dar a conocer a los servidores públicos y contratistas los lineamientos, controles y responsabilidades establecidos en el marco normativo interno de seguridad de la información de la Entidad, contribuyendo al cumplimiento de los requisitos de concienciación definidos en la norma ISO/IEC 27001:2022.

echa	Hora	Temática	Descripción	Objetivo	Nombre Tentativo	
8/03/2026	10:00 a. m.	Política General de Seguridad: Bases de nuestra defensa	Introducción a las políticas de seguridad de la información y su alineación con los objetivos estratégicos del Ministerio.	Sensibilizar sobre la importancia de las políticas y cómo forman la base de nuestra defensa contra amenazas.	¡Defiende lo Nuestro! Introducción a las Políticas de Seguridad	
2/04/2026	10:00 a. m.	¡Todos somos guardianes! Responsabilidades en Seguridad	Definir roles claros y mecanismos para garantizar el cumplimiento de responsabilidades en seguridad dentro del Ministerio.	Asegurar que cada funcionario entienda su papel en la protección de la información y cómo aportar al sistema de defensa.	¡Somos Guardianes! Responsabilidades en Seguridad de la Información	
0/05/2026	10:00 a. m.	¡Protege tus datos! Políticas y Procedimientos Clave	Estrategias de seguridad para la gestión de contraseñas, el uso de dispositivos móviles y la protección de datos personales.	Capacitar en la protección diaria de la información mediante prácticas seguras y el cumplimiento de políticas internas.	¡Protege tus Datos! Seguridad al Alcance de Todos	
4/6/2026 7/06/2025	10:00 a. m.	¡Ciberdefensa Activa! Gestión de Incidentes y Ciberseguridad	Cómo identificar, reportar y responder eficazmente ante incidentes de ciberseguridad.	Preparar al personal para detectar y actuar frente a ciberamenazas, conociendo procedimientos y recursos.	¡Ciberdefensa Activa! Responde a los Incidentes de Seguridad	Cambio de fecha
2/07/2026	10:00 a. m.	¡Tu información segura! Cifrado de Información	Cómo cifrar correos, documentos y comunicaciones para proteger datos sensibles.	Instruir en la protección avanzada de la información mediante el uso de cifrado, asegurando comunicaciones y archivos.	¡Tu Información, Tu Fortaleza! Cifrado de Datos en Acción	
6/8/2026 9/08/2026	10:00 a. m.	¡Protege tu red! Resiliencia ante DDoS	Estrategias preventivas y respuestas rápidas ante ataques de denegación de servicio (DDoS).	Enseñar cómo prevenir y mitigar los ataques DDoS, garantizando la disponibilidad de servicios críticos.	¡Protege tu Red! Resiliencia frente a Ataques DDoS	Cambio de fecha
3/09/2026	10:00 a. m.	Inteligencia Artificial: ¿Aliado o Amenaza?	Concienciar sobre los usos maliciosos de la IA, como los deepfakes, y cómo prevenir ataques automatizados.	Identificar los riesgos de la inteligencia artificial y cómo prevenir ataques que emplean IA, como deepfakes y automatización maliciosa.	¡IA: Aliado o Amenaza? Protege tus Datos	
/10/2026	10:00 a. m.	Temática pendiente a definir con el proveedor			Mes de la Seguridad: ¡Prevención y Acción!	
4/10/2026	10:00 a. m.	Temática pendiente a definir con el proveedor			Mes de la Seguridad: ¡Prevención y Acción!	
1/10/2026	10:00 a. m.	Temática pendiente a definir con el proveedor			Mes de la Seguridad: ¡Prevención y Acción!	
8/10/2026		Temática pendiente a definir con el proveedor			Mes de la Seguridad: ¡Prevención y Acción!	Por mes máximo 3 fechas. Podríamos

Imagen [14]. Cronograma y temáticas de capacitación de seguridad de la información 2026

Imagen [15]. Invitación primera charla de políticas de seguridad de la información 2026

Imagen [16]. Portada de presentación políticas de seguridad de la información

Imagen [17]. Presentación políticas de seguridad de la información