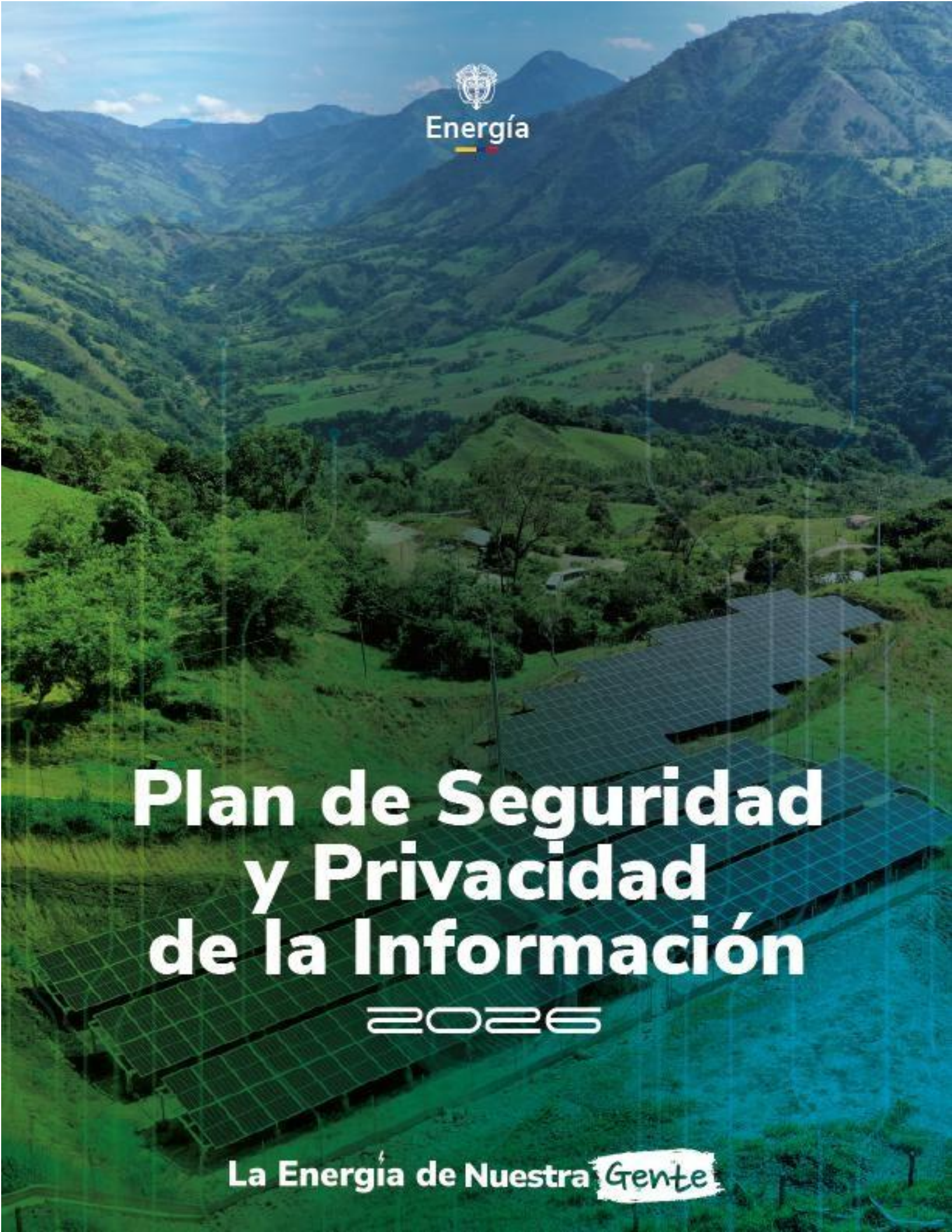

Plan de Seguridad y Privacidad de la Información

2026

La Energía de Nuestra Gente

Seguimiento Plan 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. DESCRIPCIÓN DEL INFORME

El presente informe corresponde al seguimiento del segundo trimestre (Abril–Junio 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 tercer trimestre del año.

4. PLAN OPERACIONAL DE SEGURIDAD DE LA INFORMACIÓN

4.1 Gestión de activos de información

La gestión de activos de información sigue siendo el cimiento del SGSI, en tanto permite identificar, clasificar y valorar los activos que soportan los procesos institucionales y, posteriormente, articular los resultados con el BIA, BCP, DRP, respaldos, gestión de vulnerabilidades y controles de seguridad. El plan de la vigencia definió para el segundo trimestre actividades orientadas a la entrega de información ajustada, validación y priorización de activos críticos, entrega de BIA y BCP e integración con el SGSI.

Durante el segundo trimestre se avanzó en la consolidación del inventario institucional de activos de información. De acuerdo con el seguimiento recibido, el proceso se encuentra en un nivel de avance aproximado del 90 %, quedando pendientes ocho (8) procesos de un universo de sesenta y un (61) para completar la identificación y clasificación. Este resultado refleja un avance relevante frente a la brecha identificada en 2025, aunque aún no permite declarar la matriz como cerrada o publicada oficialmente.

La información consolidada debe continuar sometiéndose a controles de calidad, revisión de consistencia, validación con responsables por dependencia y alineación con los criterios de criticidad funcional definidos para el BIA. El cierre de esta actividad es condición necesaria para fortalecer la administración de riesgos basada en activos, priorizar controles sobre servicios críticos y alimentar los planes de continuidad y recuperación ante desastres.

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

Actividad	Responsable	Periodo	Estado T2 2026	Observación
Entrega de información ajustada de activos, BIA y BCP	Responsables de dependencias	Abril 2026	En curso avanzado	Se recibieron ajustes de dependencias; se mantiene revisión de calidad y completitud.
Validación y priorización de activos críticos	Seguridad de la Información / responsables de proceso	Abril - mayo 2026	En curso	La priorización depende de la culminación de procesos pendientes y la validación de criticidad.
Integración con el SGSI	OPGI / GTIC	Junio 2026	Parcial	La integración requiere versión consolidada de la matriz y lineamientos de publicación interna.
Cierre de brechas de clasificación	GTIC / dependencias	Junio 2026	Pendiente parcial	Persisten procesos pendientes de identificación y clasificación.

4.2 Gestión de BIA y BCP

El Análisis de Impacto al Negocio (BIA) y el Plan de Continuidad del Negocio (BCP) son instrumentos esenciales para traducir la criticidad de procesos y servicios en tiempos de recuperación, recursos mínimos, procesos alternos y estrategias de continuidad. Durante el primer trimestre se había avanzado en la definición metodológica y en el levantamiento inicial de información. En el segundo trimestre, la actividad se concentró en la actualización de instrumentos institucionales y en la estructuración de insumos para el consolidado institucional.

Se reporta que la guía metodológica para la implementación del BIA se encuentra en proceso de revisión y actualización. Su propósito es fortalecer los lineamientos para identificar y valorar procesos críticos, recursos esenciales, impactos, tiempos de recuperación y procesos alternos. La guía continúa en revisión y validación por parte de la Oficina de Planeación y Gestión Internacional, por lo que su adopción formal aún debe cerrarse para garantizar aplicación homogénea en la entidad.

En cuanto a instrumentos, fueron actualizados y formalizados los formatos T-GT-F-84 - Análisis de Impacto al Negocio (BIA) y T-GT-F-85 - Plan de Continuidad del Negocio (BCP). El formato BIA incorporó mejoras en estructura, organización de servicios, activos de información, aplicaciones y recursos críticos, así como instrucciones para mejorar la consistencia del diligenciamiento. El formato BCP fue estandarizado y alineado con los resultados que se obtengan del BIA, garantizando que las estrategias de continuidad respondan a datos institucionales verificables.

También se diseñó una matriz maestra BIA consolidada para integrar la información proveniente de las dependencias, así como una estructura preliminar de informe consolidado de resultados BIA para presentar hallazgos a la PMO y a las instancias de gobierno correspondientes. Estos avances son relevantes, pero permanecen en revisión, por lo que deben cerrarse durante el tercer trimestre para que los RTO/RPO alimenten formalmente los planes de respaldo, restauración, DRP y priorización de servicios.

Tabla 2. Estado de actividades — BIA y BCP, segundo trimestre 2026

Instrumento / actividad	Estado T2 2026	Resultado	Acción pendiente
Guía de implementación BIA	En revisión	Se actualizan lineamientos metodológicos para identificación de procesos críticos, impactos y tiempos de recuperación.	Aprobación y publicación institucional.
Formato T-GT-F-84 BIA	Finalizado / formalizado	Se reestructuraron campos e instrucciones para facilitar el diligenciamiento y la consistencia.	Socialización y uso obligatorio en dependencias.
Formato T-GT-F-85 BCP	Finalizado / formalizado	Se estandarizó la estructura del plan y su alineación con resultados BIA.	Aplicación con procesos priorizados.

Matriz maestra BIA consolidada	En revisión	Se diseñó instrumento de consolidación institucional.	Validación por OPGI y cruce con activos.
Informe consolidado de resultados BIA	En estructuración	Se definió estructura preliminar de presentación de resultados.	Ajustar con resultados finales del levantamiento.

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 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, segundo 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.
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.

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

4.4 Gestión de políticas y procedimientos

Durante el segundo 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 segundo 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.

La gestión de políticas y procedimientos busca asegurar que las directrices del SGSI se encuentren documentadas, aprobadas, difundidas, implementadas y sujetas a monitoreo. Durante el primer trimestre se reportó la formalización de instrumentos relacionados con incidentes, vulnerabilidades y cifrado para transferencia de archivos. En el segundo trimestre, la gestión se orientó a mantener la formalización, promover socialización y articular estos instrumentos con los controles técnicos en operación.

Los procedimientos de monitoreo y gestión de incidentes, gestión de vulnerabilidades y cifrado de archivos internos y externos constituyen la base documental para soportar la gestión de eventos, el tratamiento de hallazgos técnicos, la protección de información sensible y la trazabilidad de acciones. Adicionalmente, la Política de Gestión de Identidades y Autenticación continúa siendo un instrumento clave para sostener la obligatoriedad de MFA y reducir el riesgo de acceso no autorizado.

4.5 Gestión de recursos de seguridad

Durante el segundo 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 xxx 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 XX nodos. Al mes de marzo, se están respaldando exitosamente XX 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

En este periodo se observa que los principales recursos técnicos que soportan la seguridad de la información se concentran en capacidades de respaldo y recuperación, seguridad perimetral, WAF, monitoreo, VPN, herramientas de gestión de vulnerabilidades, controles de identidad y

servicios asociados al nuevo modelo de continuidad. La configuración de respaldo, el hardening perimetral, el seguimiento de disponibilidad y el fortalecimiento de instrumentos BIA/BCP evidencian uso activo de recursos, pero también muestran necesidades futuras: ampliar cobertura de licenciamiento, fortalecer pruebas de restauración, sostener monitoreo continuo y preparar el ejercicio de crisis y auditoría.

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

Los indicadores del segundo trimestre permiten evaluar la eficacia de controles de disponibilidad, respaldo, continuidad, cultura, activos, BIA/BCP y monitoreo. Dado que algunos reportes técnicos contienen información sensible, el presente informe consolida los resultados a nivel ejecutivo y omite identificadores técnicos, direcciones IP, usuarios y rutas internas.

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.

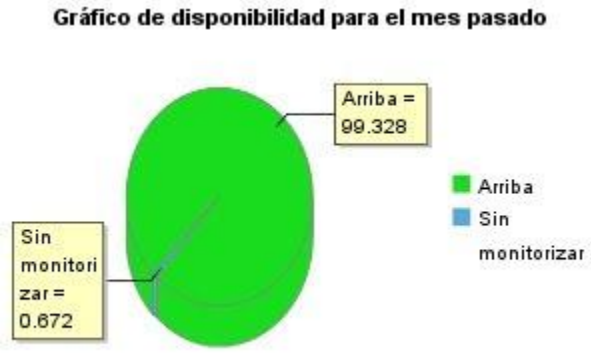

Imagen [1]. Grafico de disponibilidad firewall para el segundo trimestre 2026

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 segundo trimestre 2026

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

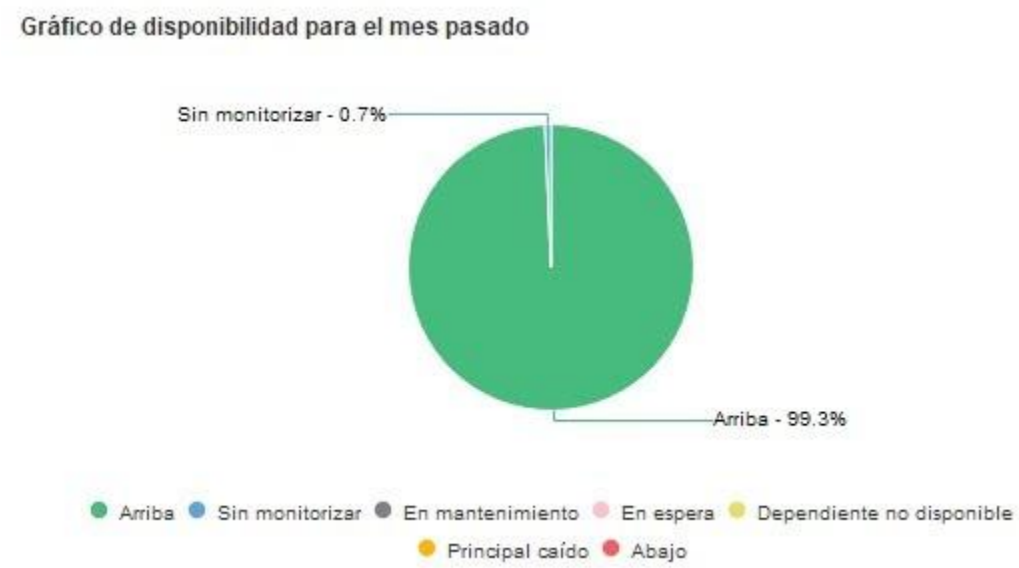

Imagen [3]. Disponibilidad WAF para el mes de Enero 2026

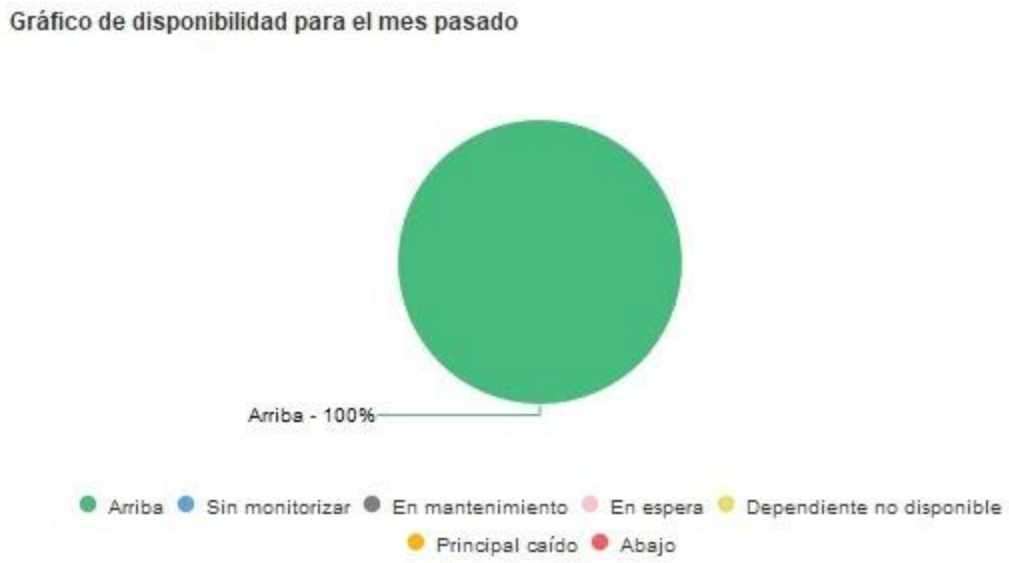

Imagen [4]. Disponibilidad WAF para el mes de abril 2026

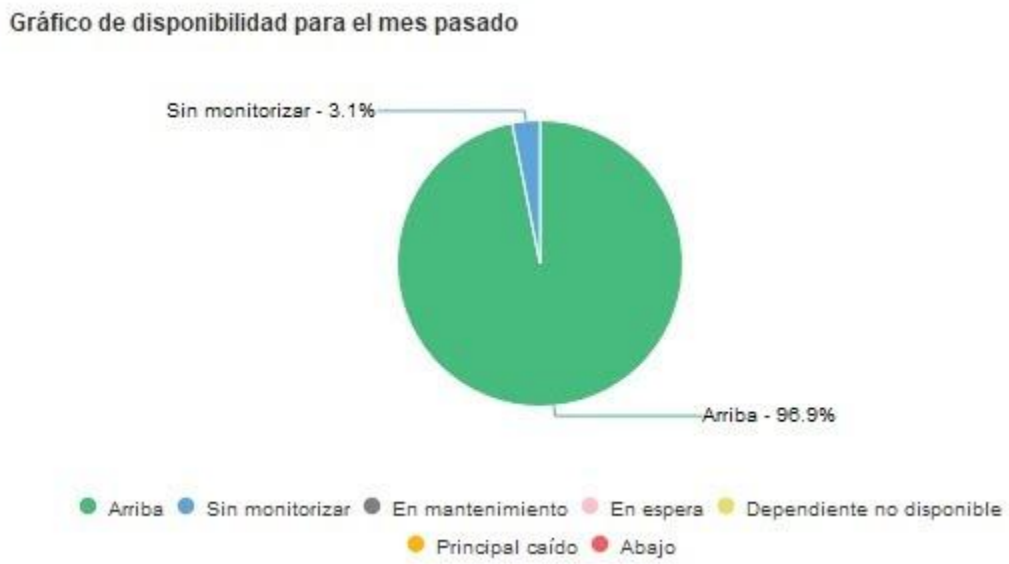

Imagen [5]. Disponibilidad WAF para el mes de Mayo 2026

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

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 segundo trimestre 2026

2. Indicadores de Protección de Endpoints :

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

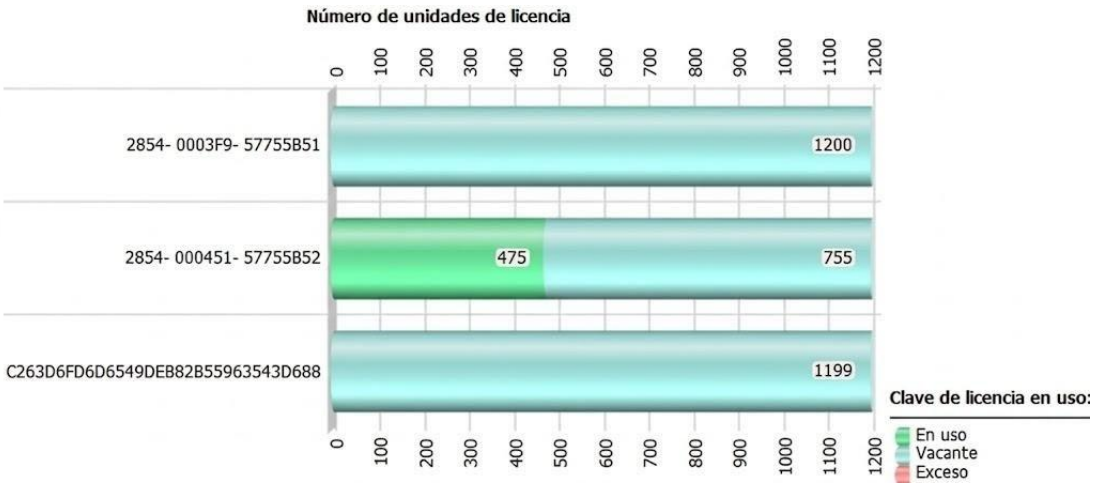

Imagen [7]. Licenciamiento de endpoints para la infraestructura de TI del Ministerio.

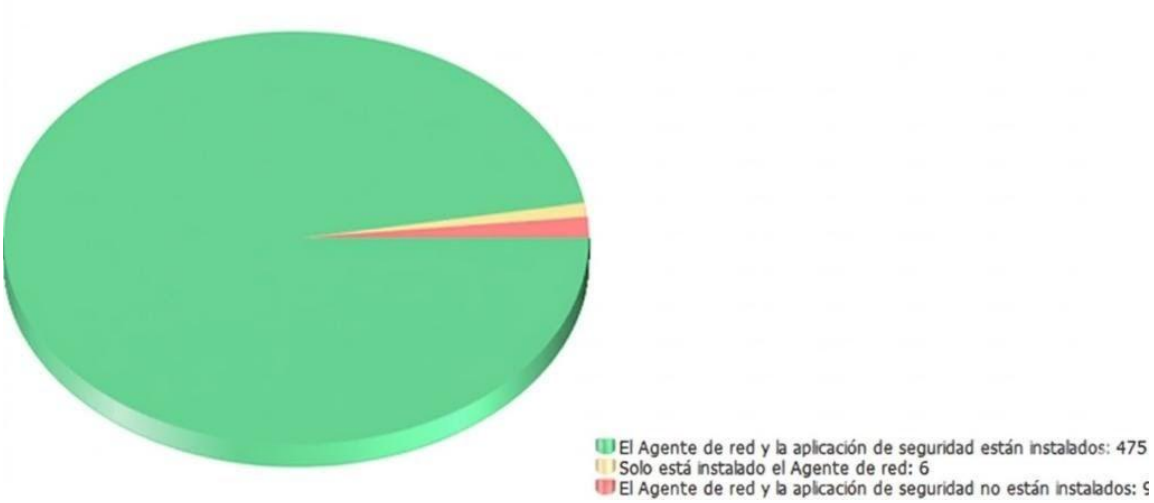

Imagen [8]. Licenciamiento de endpoints para la infraestructura de TI del Ministerio.

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

SP-149970-SAF	Hace un día	Sí		Dispositivos administrados	Crítico
SP-149997-OCI	22/01/2026 12:50:12 p. m.	Sí		Dispositivos administrados	Crítico
SP-151960-GAI	Hace 22 horas	Sí		Dispositivos administrados	Crítico
SP-151962-DVE	30/08/2024 5:51:16 p. m.	Sí		Dispositivos administrados	Crítico
SP-150746-SAF	19/12/2023 3:26:37 p. m.	Sí		Dispositivos administrados	Crítico
SP-150766-SG	19/12/2023 3:26:37 p. m.	Sí		Dispositivos administrados	Crítico
SP-150718-GIT	Hace 5 minutos	Sí	Fallo (Códig...	Dispositivos administrados	Crítico/Visible
SP-151641-STH	19/12/2023 3:26:32 p. m.	Sí		Dispositivos administrados	Crítico
SP-149946-DME	06/02/2026 8:58:39 a. m.	Sí		Dispositivos administrados	Crítico
SP-150730-STH	19/12/2023 3:26:28 p. m.	Sí		Dispositivos administrados	Crítico
SP-151577-DEE	19/12/2023 3:26:24 p. m.	Sí		Dispositivos administrados	Crítico
SP-151553-DH	06/11/2025 8:46:48 a. m.	No		Dispositivos administrados	Desconocido
SP-151507-DVM	03/10/2025 9:11:13 a. m.	No		Dispositivos administrados	Desconocido

Imagen [10]. Bloqueo de amenazas Abril-Junio 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.

Indicador	Resultado observado	Interpretación de seguridad
Disponibilidad de componentes críticos	Reportes de disponibilidad de WAF y componente XXXX muestran 100 % en las ventanas revisadas.	Comportamiento positivo para continuidad operativa y protección de aplicaciones publicadas.
Disponibilidad de enlaces de conectividad	Se evidencia recuperación en mayo frente a un evento de indisponibilidad observado en abril sobre uno de los enlaces revisados.	Debe documentarse como evento de continuidad y gestión de proveedor.
Cobertura de respaldo	Se concluyó configuración de planes en Veeam para la capacidad licenciada actual y se mantiene transición desde Arcserve.	Mejora la protección de información, pero depende de pruebas exitosas de restauración.
Pruebas de restauración	Dos pruebas controladas presentaron resultados no consistentes o fallidos.	Hallazgo crítico: requiere causa raíz, escalamiento y nuevas pruebas.
Activos de información	Avance aproximado del 90%; persisten procesos pendientes.	La matriz aún no debe considerarse cerrada oficialmente.
BIA/BCP	Formatos formalizados; guía, matriz maestra e informe consolidado en revisión.	La metodología debe aprobarse para alimentar DRP y RTO/RPO.
VPN SSL y accesos remotos	Se observan conexiones, duración agregada, volumen transferido e intentos fallidos.	Debe usarse como insumo de depuración de cuentas, MFA y alertas.
Capacitación	Tres espacios de sensibilización ejecutados.	Debe medirse participación, aprendizaje y cambios de comportamiento.

4.7 Afinamiento de la ciberseguridad

El afinamiento de la ciberseguridad durante abril-junio de 2026 evidencia un estado operativo estable de la infraestructura perimetral. El equipo principal se reporta operando normalmente, con consumo de memoria cercano al 52 % y CPU cercana al 9 %, sobre una versión estable vigente identificada en este informe como XXXX. La arquitectura opera en alta disponibilidad, sin exponer seriales, nombres de nodos, direcciones IP o identificadores internos.

Las actividades de hardening reportadas incluyen revisión de políticas, verificación de perfiles de protección web personalizados, control de modo monitor, activación de política AntiDDoS donde corresponde, depuración de políticas sin uso, actualización del WAF, depuración de usuarios locales y VPN no utilizados y bloqueo de direcciones maliciosas a partir de indicadores de compromiso de fuentes especializadas. Estas actividades disminuyen la superficie de ataque sobre aplicaciones publicadas y fortalecen la defensa frente a ataques automatizados, abuso de credenciales y explotación de vulnerabilidades web.

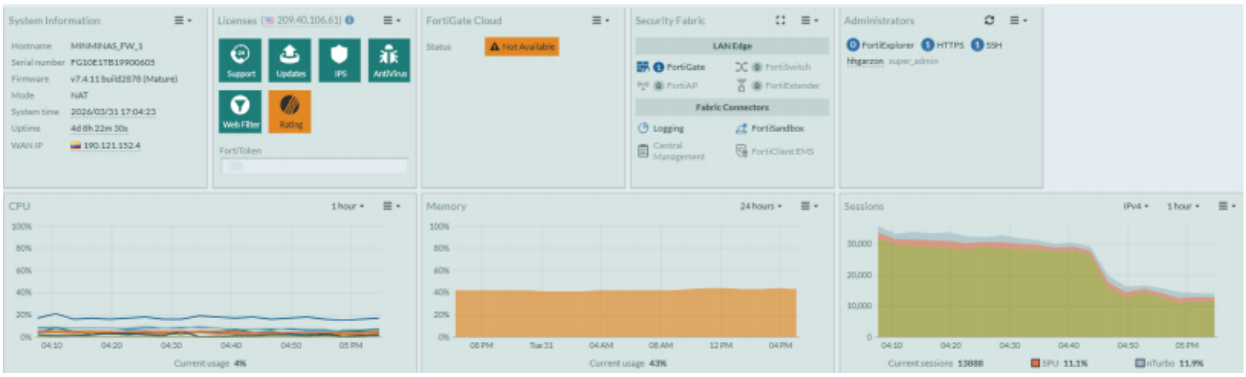

Imagen [11]. Consumo de memoria y CPU segundo trimestre 2026

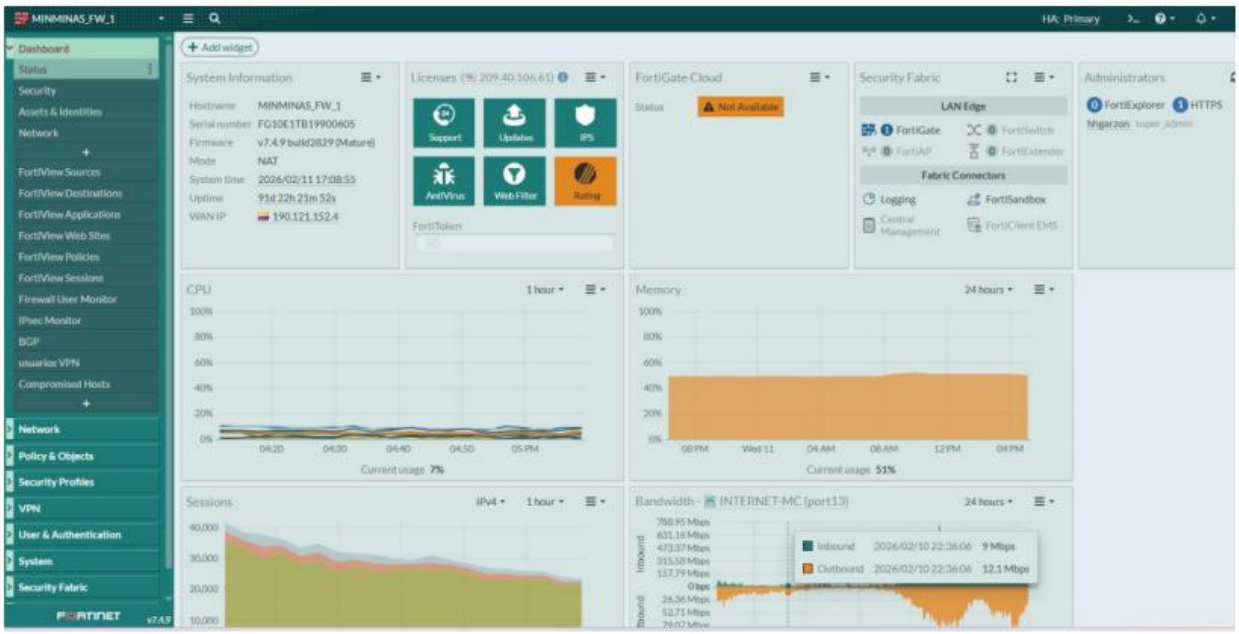

Imagen [12]. Bloqueo de amenazas segundo trimestre 2026

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

Tabla 3. Actividades de afinamiento realizadas – XXXXXXX 2026

Actividad	Estado T2	Impacto
Verificación de desempeño de firewall perimetral	Completado	Confirma operación estable y capacidad disponible.
Hardening de WAF y revisión de perfiles	Completado	Reduce exposición de aplicaciones publicadas y mejora protección web.
Depuración de políticas sin uso	Completado	Disminuye complejidad operativa y superficie de ataque.
Bloqueo de amenazas e IoC	Continuo	Fortalece respuesta preventiva frente a conexiones anómalas.
Depuración de usuarios locales y VPN	Completado / continuo	Reduce riesgo por cuentas huérfanas o innecesarias.
Mantenimiento preventivo de soluciones complementarias	Programado / en seguimiento	Sostiene disponibilidad y actualización del ecosistema de seguridad.

Fuente: Informe de Afinamiento– Abril- Junio 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

La gestión de vulnerabilidades durante el segundo trimestre mantiene dos líneas de trabajo: la formalización del procedimiento e instrumentos de seguimiento, y la ejecución de controles técnicos preventivos sobre infraestructura y aplicaciones publicadas. El procedimiento define actividades de identificación, registro, clasificación, priorización, tratamiento, verificación y seguimiento, alineadas con el control 8.8 de ISO/IEC 27001:2022 y las buenas prácticas de gestión técnica.

Durante este periodo se continuó el seguimiento a sistemas priorizados y a controles compensatorios asociados a WAF, hardening perimetral, bloqueo de amenazas y revisión previa a publicaciones. La evidencia de afinamiento indica que las aplicaciones expuestas deben mantener perfiles personalizados, reglas activas y revisiones periódicas. No obstante, el SGSI debe fortalecer la trazabilidad entre hallazgos de vulnerabilidad, plan de remediación, responsables, fecha objetivo, validación de cierre y retest.

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

APLICACIÓN	FECHA
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

APLICACIÓN	FECHA
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

APLICACIÓN	FECHA
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.

4.10 Capacitación y sensibilización

Durante el segundo trimestre se dio continuidad al cronograma de capacitación y sensibilización de seguridad y privacidad de la información. Se reporta el cumplimiento de tres espacios orientados al personal interno del Ministerio, con énfasis en herramientas frente a ciberataques, conceptos clave de seguridad de la información y ciberseguridad, ataques comunes y defensa para la protección de datos y activos de información.

Estas actividades contribuyen al riesgo transversal de cultura de seguridad digital e identidades, especialmente porque los reportes de VPN SSL evidencian intentos fallidos de autenticación y la necesidad de reforzar hábitos de acceso seguro, uso de MFA, protección de credenciales, reporte oportuno de eventos y prevención de phishing. La sensibilización debe complementarse con métricas de asistencia, evaluación de comprensión, campañas de recordación y ejercicios controlados que permitan medir reducción de comportamientos de riesgo.

Imagen [14].Capacitación 22 de abril seguridad de la información.

Imagen [15].Pieza Capacitación 22 de abril seguridad de la información.

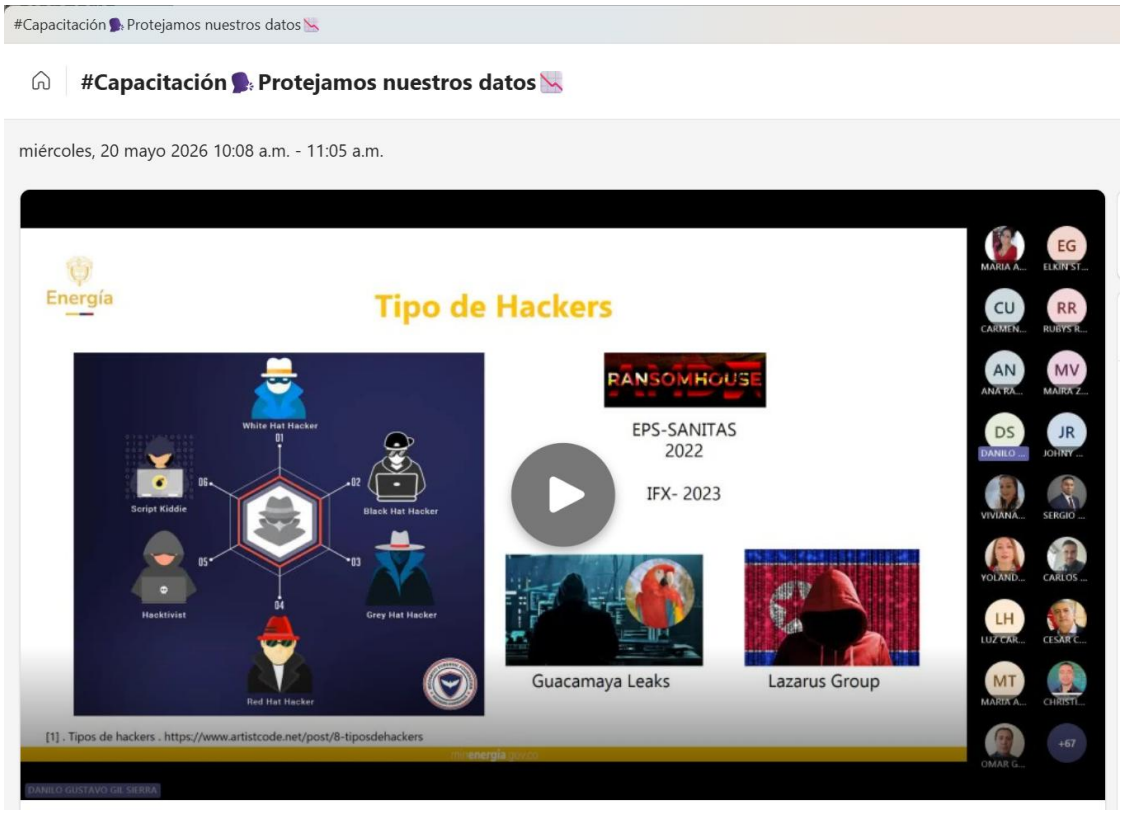

Imagen [16].Capacitación 20 de Mayo seguridad de la información.

Imagen [17].Pieza Capacitación 20 de Mayo seguridad de la información.

Imagen [18].Capacitación 17 de Junio seguridad de la información.

Imagen [19].Capacitación 17 de Junio seguridad de la información.

CONSOLIDACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Componente / actividad del Plan de Seguridad y Privacidad	Actividad principal en segundo trimestre	Estado segundo trimestre	Avance Q2	Avance acumulado anual estimado
Gestión de activos de información	Entrega de información ajustada, validación y priorización de activos críticos, integración con SGSI y cierre de brechas de clasificación.	En curso avanzado. Se reporta avance aproximado del 90% en identificación y clasificación, con procesos pendientes por cerrar.	**90%**	**45%**
Gestión de BIA y BCP	Actualización de guía BIA, formalización de formatos BIA/BCP, matriz maestra BIA e informe consolidado.	Parcial. Los formatos BIA y BCP fueron formalizados, pero la guía, matriz maestra e informe consolidado siguen en revisión.	**60%**	**35%**

Componente / actividad del Plan de Seguridad y Privacidad	Actividad principal en segundo trimestre	Estado segundo trimestre	Avance Q2	Avance acumulado anual estimado
Tratamiento de riesgos de seguridad de la información	Seguimiento articulado con riesgos priorizados, controles de IA, respaldos, continuidad, identidades y cultura.	En ejecución. Hay avances técnicos y documentales, pero persisten brechas en restauración efectiva, BIA/BCP y DRP.	**75%**	**43%**
Gestión de políticas y procedimientos	Seguimiento a procedimientos de incidentes, vulnerabilidades, cifrado y política de identidades/autenticación.	En uso y seguimiento. Los instrumentos están vigentes o en consolidación, con necesidad de socialización y medición de aplicación.	**80%**	**45%**
Gestión de recursos de seguridad	Revisión de capacidades técnicas, respaldo, seguridad perimetral, monitoreo, VPN, capacitación y continuidad.	En curso. Se evidencian recursos operando, pero se identifican necesidades de ampliación, pruebas y sostenimiento.	**70%**	**40%**
Gestión de indicadores	Consolidación de indicadores de disponibilidad, respaldo, restauración, activos, BIA/BCP, VPN y capacitación.	En curso. Existen mediciones operativas, pero se recomienda consolidarlas en tablero ejecutivo del SGSI.	**70%**	**40%**
Afinamiento de ciberseguridad	Hardening perimetral, WAF, depuración de políticas, bloqueo de amenazas, revisión de usuarios locales y VPN.	Completado para el trimestre. Las actividades reducen superficie de ataque y fortalecen defensa preventiva.	**100%**	**50%**
Plan de auditorías	Preparación del perfil del equipo auditor y definición del grupo auditor.	En preparación. La auditoría formal inicia en tercer trimestre, por lo que en Q2 solo	**50%**	**20%**

Componente / actividad del Plan de Seguridad y Privacidad	Actividad principal en segundo trimestre	Estado segundo trimestre	Avance Q2	Avance acumulado anual estimado
		aplica la etapa preparatoria.		
Gestión de vulnerabilidades	Instrumentos, priorización de activos, pruebas técnicas, planificación de remediación y retest.	En curso. Se requiere fortalecer trazabilidad entre hallazgos, responsables, fechas, cierre y retest.	**65%**	**35%**
Comunicaciones de seguridad	Difusión de políticas, procedimientos, alertas, recomendaciones y reportes de seguimiento.	En socialización y ejecución parcial. Se mantiene comunicación preventiva sin exponer información técnica sensible.	**75%**	**40%**
Capacitación y sensibilización	Tres espacios de formación sobre ciberataques, conceptos clave de seguridad, ataques comunes y protección de datos.	Ejecutado. Se recomienda medir asistencia, comprensión y cambios de comportamiento.	**100%**	**50%**

Indicador consolidado	Resultado
Avance promedio de cumplimiento de actividades programadas para Q2	**76%**
Avance acumulado estimado frente a la vigencia 2026	**40%**