



UNP



Informe

DE MONITOREO AL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Periodo monitoreado: 1 de enero al 31 de marzo de 2026.

Fecha de elaboración del documento: 28 de abril de 2026.

Direccionamiento Estratégico y Planeación
UNIDAD NACIONAL DE PROTECCIÓN
DEP-FT-11-V5
06/11/2025



 Unidad Nacional de Protección 	INFORME DE MONITOREO A PLANES INSTITUCIONALES Y ESTRATÉGICOS	 Interior 
	DIRECCIONAMIENTO ESTRATÉGICO Y PLANEACIÓN	
	UNIDAD NACIONAL DE PROTECCIÓN	

TABLA DE CONTENIDO

1. PERIODO MONITOREADO, FUENTES DE INFORMACIÓN Y SOPORTES	3
2. PRIMERA LÍNEA DE DEFENSA: RESPONSABLE DEL PLAN	3
2.1. Avance en la Implementación del Plan	3
2.2. Cumplimiento de Indicadores	3
3. SEGUNDA LÍNEA DE DEFENSA	4
3.1. Verificación Documental y Técnica de la Ejecución del Plan	4
3.2. Observaciones o Hallazgos	8
4. RECOMENDACIONES	9
5. CONCLUSIONES DEL MONITOREO	9
6. ANEXOS	10
7. CONTROL DE CAMBIOS	10



 Unidad Nacional de Protección 	INFORME DE MONITOREO A PLANES INSTITUCIONALES Y ESTRATÉGICOS	 Interior 
	DIRECCIONAMIENTO ESTRATÉGICO Y PLANEACIÓN	
	UNIDAD NACIONAL DE PROTECCIÓN	

1. PERIODO MONITOREADO, FUENTES DE INFORMACIÓN Y SOPORTES

El periodo monitoreado corresponde al primer trimestre de 2026, comprendido entre el 1 de enero y el 31 de marzo, en coherencia con la hoja de ruta definida para el presente plan.

Las fuentes de información empleadas para el desarrollo del monitoreo incluyeron el Plan de Seguridad y Privacidad de la Información 2026, las evidencias documentales aportadas por la Oficina de Tecnologías y Sistemas de Información - OTSI, la Hoja de Ruta del Plan y el Informe de Monitoreo de Primera Línea de Defensa.

Para el desarrollo del monitoreo, se efectuó la revisión de las siguientes fuentes de información:

- 01. Constancia Secretarial
- Acta de reunión
- Archivo autodiagnóstico
- GTE-FT-05-V5 Informe de Estado y Gestión pruebas
- Informe Técnico de Análisis de vulnerabilidades de Infraestructura (PT-013...)
- GTE-FT-05-V5 Informe de Estado y Gestión Pentesting.
- GTE-FT-05-V5 Informe de Estado y Gestión Prueba.
- GTE-FT-05-V5 Informe de Inteligencia de Amenazas.

A partir del acceso al repositorio digital, la verificación se fundamentó en la revisión de evidencias digitales suministradas por el proceso responsable del Plan, tales como matriz estructurada, informes y acta. Desde la Segunda Línea de Defensa se verificó la calidad, consistencia y suficiencia de estos soportes, con el fin de confirmar la trazabilidad de la información y la efectiva ejecución de las acciones programadas. Este ejercicio permitió identificar oportunidades de mejora, fortalecer los mecanismos de control y generar recomendaciones orientadas a optimizar la gestión de la seguridad y privacidad de la información en la Entidad.

2. PRIMERA LÍNEA DE DEFENSA: RESPONSABLE DEL PLAN

2.1. Avance en la Implementación del Plan

“NO APLICA”.

2.2. Cumplimiento de Indicadores

“NO APLICA”.



3. SEGUNDA LÍNEA DE DEFENSA

Se deja constancia formal de las actividades de Monitoreo realizadas sobre las evidencias documentales digitales suministrada por el proceso responsable del Plan de Seguridad y Privacidad de la Información correspondiente al primer trimestre de 2026.

3.1. Verificación Documental y Técnica de la Ejecución del Plan

La verificación documental y técnica de la ejecución del Plan se desarrolló a partir de un proceso sistemático de verificación, análisis y contraste de la información reportada por la primera línea de defensa frente actividades definidas en la Hoja de Ruta para el primer trimestre. Este ejercicio incorporó los criterios establecidos en el Manual para la formulación, ejecución y monitoreo de planes.

El proceso de validación se centró en la evaluación técnica de los soportes documentales, verificando atributos como la suficiencia, consistencia, integridad, actualidad y alineación con los lineamientos definidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) y la planificación institucional. Asimismo, se revisó la correspondencia entre las evidencias presentadas y los entregables esperados, con el fin de confirmar la efectiva ejecución de las actividades.

Como resultado, se consolidó la *Matriz de Verificación Documental y Técnica de la Ejecución del Plan 1 trimestre 2026*, la cual constituye un instrumento de control que integra el detalle de las actividades verificadas, los soportes documentales y su convalidación. En la Matriz se registra el estado de cada actividad la fecha de generación de la evidencia o expedición del documento y su ubicación, garantizando trazabilidad, disponibilidad y consulta de la información.

Tabla Matriz de Verificación Documental y Técnica de la Ejecución del Plan 1 trimestre.

Objetivo	Fases	Tipo de documento (entregable)	Mes y año	Fuente/ Enlace	Cumple (Si/No, Parcial)	Observaciones
Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la Entidad.	Aprobación del Plan de Seguridad de la Información por el Comité Institucional de Gestión y Desempeño.	Constancia secretarial (.Pdf).	Enero 2026	Repositorio Digital OTSI.	Si.	Evidencia presentada sustentada. y
	Realizar la evaluación con la herramienta de autodiagnóstico de MinTic.	Archivo autodiagnóstico (.xlsx) Acta de reunión (.Pdf).	Marzo 2026 Febrero 2026	Repositorio Digital OTSI.	Si	Evidencia presentada sustentada. y
	Realizar un análisis de vulnerabilidades de infraestructura.	Informe de Estado y Gestión "Evaluación de Seguridad". (.Pdf). Anexo Informe de proveedor (PT-013...) (.pdf).	Febrero 2026	Repositorio Digital OTSI.	SI	Evidencia presentada sustentada. y



Objetivo	Fases	Tipo de documento (entregable)	Mes y año	Fuente/ Enlace	Cumple (Si/No, Parcial)	Observaciones
	Realizar un análisis de vulnerabilidades de Sistemas de Información	GTE-FT-05-V5 Informe de Estado y Gestión Pentesting. (.pdf). GTE-FT-05-V5 Informe de Estado y Gestión Prueba (.pdf).	Marzo 2026	Repositorio Digital OTSI.	Si	Evidencia presentada sustentada. y
	Realizar un análisis de inteligencia de amenazas.	GTE-FT-05-V5 Informe de Estado y Gestión - Inteligencia de Amenazas (.pdf).	Marzo 2026	Repositorio Digital OTSI.	Si.	Evidencia presentada sustentada. y

Fuente: Elaboración propia a partir de la documentación proporcionada

Una vez obtenida la matriz de verificación documental, se presenta la validación técnica de las evidencias y el análisis de cada una frente al indicador de medición evidenciado en el Plan.

Indicador de Medición.

Cumplimiento del Plan Seguridad y Privacidad de la información = $\frac{\text{Fases ejecutadas durante el trimestre}}{\text{Fases programadas durante el trimestre}} * 100$

- **Avance esperado del trimestre:** 30%
- **Meta anual:** 100%

A partir de la estructura definida, se desprende el análisis técnico para cada una de las fases:

Aprobación del Plan de Seguridad de la Información por el Comité Institucional de Gestión y Desempeño

Se dispone de evidencia formal del proceso de aprobación del Plan de Seguridad de la Información para la vigencia 2026, a través de la Constancia Secretarial fechada el 23 de enero de 2026, debidamente suscrita por el Secretario Técnico Comité Institucional de Gestión y Desempeño – UNP/ Jefe Oficina Asesora de Planeación, Javier Francisco Rodríguez Moreno y cargada en el repositorio digital. La constancia constituye el soporte registrado en la Hoja de Ruta que respalda el cumplimiento del requisito de aprobación del Plan en comento.

La actividad se encuentra cumplida al 100%, aportando el 6% al cumplimiento del 30% de la meta trimestral establecida.



Ilustración 1 Extracto del encabezado de la Constancia Secretarial enero 2026

CONSTANCIA SECRETARIAL		
En ejercicio de las funciones establecidas en el artículo 5° de la Resolución 791 de 2024		
HACE CONSTAR		
Que en la primera sesión extraordinaria desarrollada de manera presencial realizada el 23 de enero de 2026 se presentó y aprobó		
Item	Asunto - Aprobación	Responsable
5	Actualización y Aprobación de planes, programas y proyectos: (Plan Estratégico Institucional- PEI 2023-2026 (actualización) Plan de Acción Institucional PAI 2026- Integración de planes (Decreto 612 de 2018 y otras fuentes normativas), Plan Operativo	Javier Francisco Rodríguez Moreno (Jefe Oficina Asesora)

Fuente: Oficina de Tecnologías y Sistemas de Información (2026).
Constancia Secretarial del Comité Institucional de Gestión y Desempeño

Realizar la evaluación con la herramienta de autodiagnóstico de MinTic.

De acuerdo con la revisión efectuada, se evidencia el archivo en formato Excel correspondiente a la evaluación de autodiagnóstico con corte a marzo de 2026. Asimismo, se cuenta con el acta de reunión de febrero de 2026, en la cual se llevó a cabo una mesa de trabajo con el fin de evaluar controles, entre otros aspectos.

En este sentido, la evidencia aportada permite acreditar el cumplimiento integral de la actividad, configurándose un cumplimiento total desde la perspectiva de verificación documental.

La actividad se encuentra cumplida al 100%, aportando el 6% al cumplimiento del 30% de la metra trimestral establecida.

Realizar un análisis de vulnerabilidades de infraestructura

De la revisión a la evidencia aportada, se verificó la ejecución de una evaluación de seguridad bajo enfoque de caja negra. El Informe Técnico de febrero de 2026 muestra el objetivo, alcance y aspectos relevantes de la evaluación de seguridad sobre un sitio en específico, así como la actividad desarrollada, la gestión realizada, la descripción de los hallazgos y las recomendaciones para subsanar.

El informe se encuentra suscrito por el especialista en Ciberseguridad, un colaborador apoyo técnico de la Oficina de Tecnología y la aprobación formal del Jefe (E) de la Oficina de Tecnologías y Sistemas de Información, responsable del proceso, con el respectivo anexo técnico. En Consecuencia, la evidencia corresponde a una evaluación externa de vulnerabilidades con cierre formal.



 Unidad Nacional de Protección 	INFORME DE MONITOREO A PLANES INSTITUCIONALES Y ESTRATÉGICOS	 Interior 
	DIRECCIONAMIENTO ESTRATÉGICO Y PLANEACIÓN	
	UNIDAD NACIONAL DE PROTECCIÓN	

La actividad se encuentra cumplida al 100%, aportando el 6% al cumplimiento del 30% de la metra trimestral establecida.

Realizar un análisis de vulnerabilidades de Sistemas de Información

De acuerdo con la revisión documental, se evidenció la entrega de dos Informes de Estado y Gestión denominados “*GTE-FT-05-V5 Informe de Estado y Gestión Pentesting*” y “*GTE-FT-05-V5 Informe de Estado y Gestión Prueba*”, los cuales contienen el detalle de las pruebas realizadas, información general del proceso, así como los riesgos asociados, las alternativas de solución, recomendaciones y conclusiones orientadas a la subsanación de hallazgos.

Adicionalmente, se observa que los Informes se encuentran suscritos por un colaborador de Ciberseguridad, un colaborador apoyo técnico de la Oficina de Tecnología y el Jefe (E) de la Oficina de Tecnologías y Sistemas de Información. En consecuencia, la evidencia aportada permite acreditar un cumplimiento desde la perspectiva de verificación documental.

La actividad se encuentra cumplida al 100%, aportando el 6% al cumplimiento del 30% de la metra trimestral establecida.

Informe de Inteligencia de Amenazas

Conforme la revisión documental, se evidenció la entrega “*El informe de Estado y Gestión Inteligencia de Amenazas...*” en formato pdf, en el cual se abordó un caso relacionado con Phishing, incluyendo el objetivo y alcance del informe, las actividades desarrolladas y las recomendaciones para el caso. El contenido incorpora además elementos relacionados con la realización de una campaña remitida a través de correo electrónico en marzo de 2026.

Adicionalmente, se observa que los Informes se encuentran suscritos por un colaborador de Ciberseguridad, un colaborador apoyo técnico de la Oficina de Tecnología y el Jefe (E) de la Oficina de Tecnologías y Sistemas de Información. En consecuencia, la evidencia aportada permite acreditar un cumplimiento desde la perspectiva de verificación documental.

La actividad se encuentra cumplida al 100%, aportando el 6% al cumplimiento del 30% de la metra trimestral establecida.

De acuerdo con lo expresado en el indicador del Plan, el resultado del primer trimestre de 2026 se representa de la siguiente forma:

Respecto del 100,



Cumplimiento del Plan Seguridad y Privacidad de la información = $\frac{\text{Fases ejecutadas durante el trimestre}}{\text{Fases programadas durante el trimestre}} * 100$

$$= \frac{5}{5} * 100$$

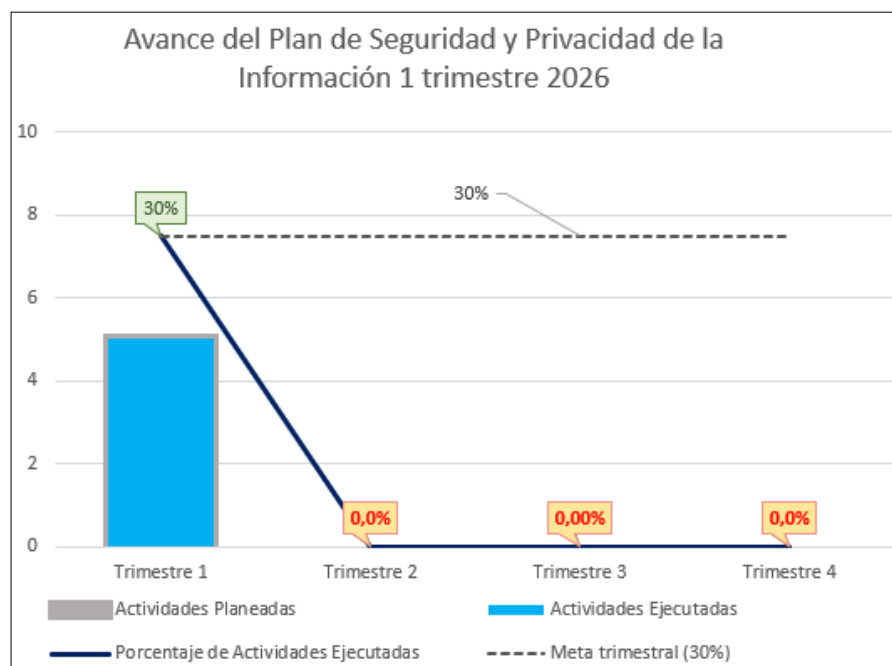
= 100% del total de cumplimiento del Plan.

Respecto del 30% para el trimestre,

$$= 100\% * 30\% = 30\% \text{ del total de cumplimiento del Plan.}$$

Por lo tanto, a cierre del primer trimestre la Meta alcanzada del Plan se representa de la siguiente forma:

Ilustración 2 Estado del Plan de Seguridad y privacidad de la Información



Fuente: Elaboración propia con base en datos del informe de Monitoreo de Segunda Línea de Defensa

3.2. Observaciones o Hallazgos

Desde el enfoque de monitoreo de segunda línea de defensa, se realizó la verificación de todas las actividades del Plan, sin evidenciarse observaciones o hallazgos frente a su cumplimiento.



 Unidad Nacional de Protección	INFORME DE MONITOREO A PLANES INSTITUCIONALES Y ESTRATÉGICOS	 Interior
	DIRECCIONAMIENTO ESTRATÉGICO Y PLANEACIÓN	
	UNIDAD NACIONAL DE PROTECCIÓN	

En la revisión efectuada, se reconoce la ejecución de las pruebas y la existencia de la documentación soporte correspondiente, la cual se encuentra alineada con lo establecido para la actividad en la Hoja de Ruta.

En consecuencia, no se generan recomendaciones adicionales en el marco del presente monitoreo, al evidenciarse consistencia en la información revisada.

4. RECOMENDACIONES

Desde la Segunda Línea de Defensa se recomienda:

Es necesario realizar seguimiento prioritario a la subsanación de los hallazgos identificados y suscritos en los informes de Estado y Gestión, asegurando su cierre efectivo y documentado.

Asegurar la validación y aprobación formal por parte del responsable del proceso como condición para considerar cumplidos los entregables, mitigando riesgos de reprocesos y desalineación con la necesidad.

5. CONCLUSIONES DEL MONITOREO

- Balance general del cumplimiento del plan:

Durante el primer trimestre de 2026, el Plan de Seguridad y Privacidad de la Información refleja un estado porcentual del 30% del 30% proyectado para el trimestre. Esto es, las cinco (5) actividades ejecutadas durante la vigencia monitoreada, de conformidad con el cronograma establecido y los soportes documentales aportados.

En conclusión, desde una perspectiva técnica, se evidencia el cumplimiento del plan establecido y del indicador correspondiente al primer trimestre de 2026. La ejecución de las actividades programadas se desarrolló conforme a los lineamientos definidos, asegurando la disponibilidad de la información soporte.

- Observaciones estratégicas.

Se destaca que el cumplimiento planeado del 30% del plan y del indicador definido evidencia un desempeño satisfactorio y alineado con los objetivos establecidos, lo cual refleja una gestión efectiva durante el periodo evaluado.

A partir de este resultado, se recomienda fortalecer los mecanismos de seguimiento y trazabilidad documental, de manera que no solo se conserve el nivel de cumplimiento alcanzado, sino que también se potencie la capacidad de análisis del desempeño, la minimización de riesgos, la trazabilidad documental y la toma de decisiones basada en información consolidada.

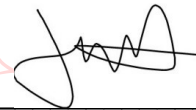


6. ANEXOS

Con el fin de garantizar la trazabilidad, veracidad y respaldo de la información consignada en el presente informe, se relacionan como soporte los documentos descritos en la tabla denominada *Matriz de Verificación Documental y Técnica de la Ejecución del Plan 1 trimestre*, los cuales respaldan la ejecución consignada en el presente informe.

Archívese en: Seguimiento a planes institucionales de acuerdo con la Tabla de Retención Documental del proceso de Direccionamiento Estratégico y Planeación DEP. TRD 1030

Firmado digitalmente
por Javier Francisco
Rodríguez Moreno



Javier Francisco Rodríguez Moreno
Jefe Oficina Asesora de Planeación

	Nombre	Firma	Fecha
Proyectó	Maria Eugenia Navarrete Forero		28/04/2026
Revisó	Belly Ovalle Alarcon		
Aprobó	Javier Francisco Rodríguez Moreno		

Los arriba firmantes declaramos que hemos revisado el presente documento y verificamos que su contenido se ajusta a las disposiciones normativas y metodológicas vigentes. En consecuencia, lo suscribimos bajo nuestra responsabilidad para los fines institucionales correspondientes.

7. CONTROL DE CAMBIOS

VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
00	Se crea el documento como lo establece el Manual Formulación y seguimiento a Planes	06/11/2020	01
01	Se realiza la modificación de acuerdo con el MEM22-00033953 Lineamiento de imagen nuevo gobierno y así mismo teniendo en cuenta la Resolución 1366 de 2022 se traslada al proceso de Direccionamiento Estratégico y Planeación	21/10/2022	02
02	Se realiza la actualización de logos de acuerdo con la imagen del nuevo Gobierno.	23/08/2023	03
03	Se realiza la actualización de logos de acuerdo con el Manual de Identidad Visual	17/10/2024	04
04	Actualización de la estructura general del informe conforme a los nuevos lineamientos del manual de formulación, ejecución y monitoreo de planes institucionales y estratégicos (DEP-MA-02). También se cambia el nombre y enfoque del informe para mantener la alineación con los lineamientos del manual.	06/11/2025	05

