Instituto Nacional de Metrología de Colombia

Plan Estratégico de Seguridad y Privacidad de la Información (PESI)

2024-2026

OIDT

Bogotá, enero de 2026

INTRODUCCIÓN

El Plan Estratégico de Seguridad y Privacidad de la Información del Instituto Nacional de Metrología se formula como el instrumento orientador para la implementación, operación, seguimiento y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información (SG-SPI), en coherencia con la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y las mejores prácticas nacionales e internacionales en la materia.

Este Plan se fundamenta en la recopilación, análisis y articulación de los lineamientos normativos, políticas, estándares y buenas prácticas aplicables en seguridad de la información y protección de datos personales, con el propósito de establecer los requisitos necesarios para el diagnóstico del estado actual, la planificación estratégica, la implementación de controles, la gestión de riesgos y el mejoramiento continuo del MSPI. En este marco, se definen políticas, procedimientos y controles eficaces, alineados con la estrategia institucional del INM, orientados al tratamiento de los riesgos de seguridad digital y de protección de datos personales.

El Plan contempla la adopción de metodologías para la identificación, clasificación y valoración de los activos de información, así como para la evaluación y el tratamiento de los riesgos, como mecanismos esenciales para prevenir, mitigar y controlar los impactos sobre la confidencialidad, integridad, disponibilidad y privacidad de la información, considerando los efectos potenciales para la entidad, los titulares de la información y las demás partes interesadas.

Asimismo, el Plan establece mecanismos de seguimiento, medición y evaluación de la eficacia de los controles implementados, apoyados en programas de auditoría, revisiones periódicas por la Alta Dirección y la gestión sistemática de no conformidades, incidentes y oportunidades de mejora, garantizando la sostenibilidad y mejora continua del sistema.

Para su desarrollo, se realiza un análisis de la situación actual y del estado objetivo en materia de seguridad y privacidad de la información, a partir del cual se definen las estrategias, proyectos, actividades, responsables, cronogramas y recursos necesarios para fortalecer progresivamente el nivel de madurez institucional. Todo ello con el fin de asegurar una protección adecuada de los activos de información del INM, garantizar el cumplimiento del marco normativo vigente, mitigar los riesgos de seguridad digital y contribuir a la continuidad de la operación y a la confianza de las partes interesadas.

En síntesis, el Plan Estratégico de Seguridad y Privacidad de la Información constituye un pilar fundamental para la gestión integral de la información del INM, al articular la seguridad, la privacidad y la gestión del riesgo como habilitadores estratégicos para el cumplimiento de los objetivos misionales y la prestación eficiente de los servicios institucionales.

1. OBJETIVO GENERAL

Optimizar el Plan de Seguridad y Privacidad de la Información del INM mediante la implementación, operación, seguimiento y mejora continua de los controles de seguridad de la información definidos en la norma ISO/IEC 27001:2022 (Anexo A) y en el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio TIC, en articulación con la estrategia de Gobierno Digital, con el fin de gestionar adecuadamente los riesgos de seguridad digital y garantizar la confidencialidad, integridad y disponibilidad de la información institucional durante la vigencia 2024–2026.

1.1. OBJETIVOS ESPECÍFICOS

- Identificar, analizar y valorar los riesgos de seguridad de la información y de protección de datos personales asociados a los activos de información y a los tratamientos realizados por el INM, con el fin de priorizar la implementación de controles técnicos, administrativos y organizacionales conforme a ISO/IEC 27001:2022, el MSPI y la normativa de protección de datos personales.

- Definir, actualizar y homologar el marco de controles de seguridad de la información y protección de datos personales, articulando los controles del Anexo A de la ISO/IEC 27001:2022 con los lineamientos del MSPI y los principios, deberes y obligaciones establecidos en la Ley 1581 de 2012, en alineación con la estrategia de Gobierno Digital.

- Implementar los controles de seguridad de la información y de protección de datos personales priorizados, garantizando su aplicación efectiva en los procesos, sistemas de información y servicios institucionales, para salvaguardar la confidencialidad, integridad, disponibilidad y privacidad de la información y de los datos personales tratados por el INM.

- Establecer, mantener y actualizar la documentación del Sistema de Gestión de Seguridad y Privacidad de la Información, incluyendo políticas, procedimientos, avisos de privacidad, cláusulas de tratamiento, inventarios y registros de bases de datos personales, que soporten la gestión integral de la seguridad de la información y la protección de datos personales.

- Fortalecer las capacidades institucionales en seguridad de la información y protección de datos personales, mediante programas de sensibilización, capacitación y apropiación de controles por parte de servidores públicos, contratistas y terceros que realicen tratamiento de información o datos personales del INM.

- Realizar el seguimiento, medición y evaluación de la eficacia de los controles de seguridad de la información y protección de datos personales, a través de indicadores, auditorías, revisiones y mecanismos de supervisión, que permitan verificar el cumplimiento normativo y el desempeño del sistema.

- Gestionar de manera oportuna los incidentes de seguridad de la información y los eventos relacionados con datos personales, incluyendo la atención de incidentes, brechas de seguridad y posibles vulneraciones de derechos de los titulares, definiendo e implementando acciones correctivas, preventivas y de mejora continua.

- Asegurar la articulación del Plan de Seguridad y Privacidad de la Información y del régimen de protección de datos personales con el Sistema Integrado de Gestión (SIG), garantizando coherencia institucional, cumplimiento de requisitos legales y fortalecimiento del control interno.

2. ALCANCE

El Plan Estratégico de Seguridad y Privacidad de la Información del INM tiene como alcance la implementación, operación, seguimiento y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información (SG-SPI) y de la estrategia institucional de seguridad digital, en concordancia con la Política General de Seguridad de la Información del INM, la cual establece la cobertura de todos los procesos, dependencias, sistemas de información, activos de información y tratamientos de datos personales de la entidad.

El Plan comprende la gestión integral de la seguridad de la información y la protección de datos personales, incorporando controles técnicos, administrativos y organizacionales alineados con la norma ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio TIC y la normativa colombiana vigente en materia de protección de datos personales. Su ejecución abarca la identificación y valoración de riesgos, la definición e

implementación de controles, la gestión de incidentes, el fortalecimiento de capacidades institucionales y la evaluación permanente de la eficacia del sistema.

El Plan inicia con el diagnóstico del estado actual de la seguridad de la información y la protección de datos personales en el INM, continúa con la formulación y ejecución de los proyectos asociados a cada eje estratégico de seguridad digital y privacidad, y finaliza con la definición del cronograma, los responsables y el presupuesto requerido, garantizando la trazabilidad, sostenibilidad y articulación con el Sistema Integrado de Gestión (SIG) durante la vigencia establecida.

3. ABREVIATURAS O SÍMBOLOS

INM: Instituto Nacional de Metrología

MinTic: Ministerio de las telecomunicaciones

SGSI: Sistema de gestión de seguridad de la información

PESI: Plan Estratégico de seguridad de la información

4. DEFINICIONES

- **Activos**

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Control**

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Riesgo**

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información**

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI**

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000.

5. MARCO NORMATIVO

- Constitución Política de Colombia – Artículo 15: Derecho fundamental a la intimidad, al habeas data y a la protección de datos personales.
- Ley 1581 de 2012
- Decreto 1377 de 2013 y Decreto 1074 de 2015
- Ley 1712 de 2014
- Decreto 1078 de 2015
- Decreto 1008 de 2018
- Resolución 1519 de 2020 – MinTIC
- Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC
- Decreto 612 de 2018
- Resolución 500 de 2021.
- Ley 44 de 1993
- Ley 1273 de 2009
- Ley 527 de 1999
- Ley 594 de 2000
- Ley 850 de 2003
- Ley 1266 de 2008
- Ley 1341 de 2009
- Ley 1437 de 2011

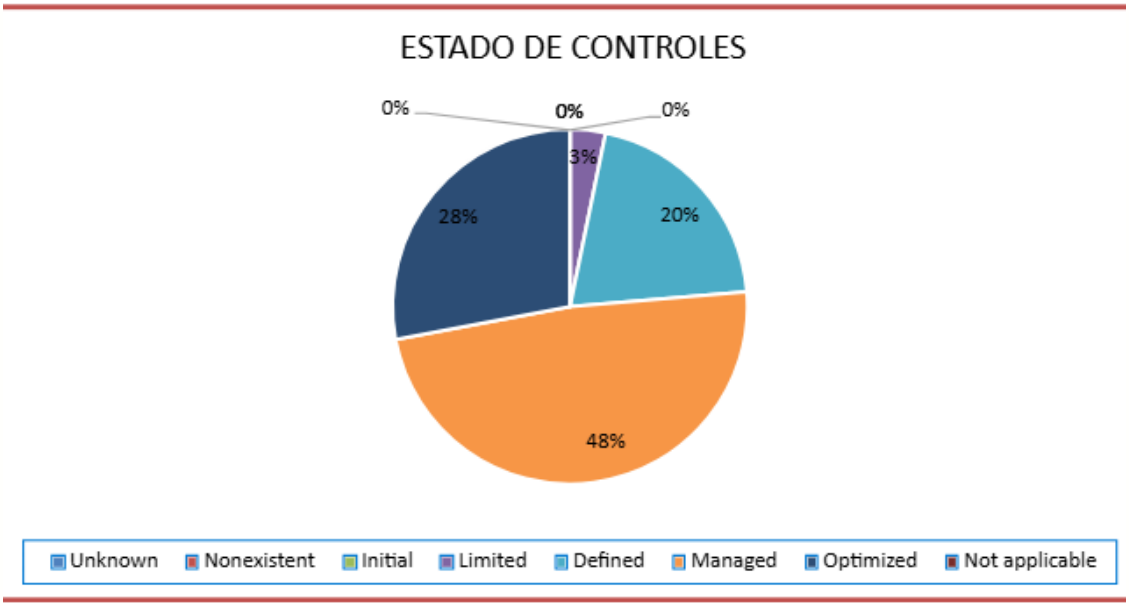
- Ley 1474 de 2011
- Ley 1915 de 2018
- Ley 1952 de 2019
- Decreto 2609 de 2012
- Decreto 0884 de 2012
- Decreto 886 de 2014
- Decreto 103 de 2015
- Decreto 1080 de 2015
- Decreto 1081 de 2015
- Resolución 512 de 2019
- Resolución 1519 de 2020
- Directiva 03 de 2021
- CONPES 3701 de 2011
- CONPES 3854 de 2016
- Manual de Gobierno Digital – MINTIC.
- NTC/ISO 27001:2022

6. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La seguridad y privacidad de la información, es un componente transversal a la Estrategia de Gobierno en línea. Este va alineado con la implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos del INM.

El INM ha avanzado en la implantación de este modelo de seguridad y el objetivo es seguir madurándolo en la vigencia 2024-2026, cumpliendo con el ciclo del modelo de seguridad y privacidad de la información, donde se enfatiza en una mejora continua. Este modelo se está implantando apoyado también en el estándar de seguridad ISO 27001:2022.

Estado del SGSI basado en el avance de implementación de los controles ISO27001:2022 a diciembre 2025



Los criterios de medición son los siguientes:

ISO/IEC 27001:2022 ISMS	
Estado	**Criterio**
No Aplica	No aplica
Inexistente	Falta total de políticas, procedimientos, controles, etc. reconocibles.
Inicial	El desarrollo apenas ha comenzado y requerirá un trabajo significativo para cumplir con los requisitos.
Limitado	Se ha hecho algún progreso, pero aún no se ha completado su implementación.
Definido	El control está definido o documentado, aunque faltan detalles y/o aún no se implementa
Administrado	El desarrollo está completo, el proceso/control ha sido implementado, documentado y está operando
Optimizado	El requerimiento se cumple completamente, está operando completamente como se esperaba, se está monitoreando y mejorando activamente, y hay evidencia sustancial para demostrar todo eso a los auditores.

A partir del análisis de los diagnósticos realizados, se proyecta que la totalidad de los controles de seguridad y privacidad de la información evolucionen progresivamente hacia niveles de madurez administrado y optimizado. En este contexto, el INM evidencia un avance significativo en el fortalecimiento de su Sistema de Gestión de Seguridad de la Información (SGSI), reflejando una tendencia positiva hacia la consolidación de estos niveles óptimos de madurez.

Hasta la vigencia 2025, el INM ha desarrollado acciones sistemáticas orientadas al fortalecimiento del SGSI, mediante la adopción e implementación de procedimientos, instructivos, campañas de sensibilización en seguridad de la información y otras prácticas de gestión. Como resultado, se ha alcanzado un nivel de madurez relevante en los siguientes dominios y controles:

- Políticas de seguridad de la información
- Gestión de activos de información
- Control de accesos
- Gestión de incidentes de seguridad de la información
- Seguridad en el desarrollo de software
- Seguridad en redes

- Gestión de copias de seguridad (backups)
- Documentación de la operación de la OIDT
- Gestión de la capacidad
- Gestión de riesgos de seguridad de la información
- Controles tecnológicos antimalware

No obstante, persisten controles que requieren fortalecimiento y desarrollo, los cuales constituyen el foco estratégico del Plan formulado en el presente documento. Lo anterior se realizará sin detrimento del mantenimiento, seguimiento y mejora continua de aquellos controles que actualmente se encuentran en niveles de madurez administrado y optimizado, con el fin de asegurar la sostenibilidad, eficacia y evolución permanente del sistema.

7. ESTRATEGIA DE SEGURIDAD DIGITAL

EL INM establece una estrategia de seguridad digital en la que integra los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira en torno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y el procedimiento de gestión de incidentes que ha establecido. Adicionalmente el INM trabaja en su SGSI basado en el estándar de seguridad ISO27001:2022.

Por tal motivo, el INM enfoca su PESI en los siguientes 8 ejes, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

8. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, según MSPI y la resolución 500 de 2021:

a. Gobierno y Direccionamiento de la Seguridad y Privacidad de la Información

El objetivo del eje es consolidar el liderazgo institucional, la gobernanza y la toma de decisiones en seguridad y privacidad de la información, asegurando la articulación del MSPI con la estrategia institucional, el Sistema Integrado de Gestión y la Política de Gobierno Digital.

b. Gestión Integral de Riesgos de Seguridad y Privacidad de la Información

Tiene como finalidad la gestión de forma sistemática los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información, priorizando acciones preventivas y planes de tratamiento acordes con el contexto institucional. Se tiene como objetivo implementar una metodología teniendo en cuenta la guía emitida por la función pública y en conjunto con la Oficina Asesora de Planeación se generará un plan de trabajo para iniciar su implementación. La definición y metodología para este eje se encuentra establecida en el Plan de Tratamiento de Riesgos de Seguridad de la Información, el cual se anexa al presente documento.

c. Implementación y Operación de Controles de Seguridad de la Información

Para la vigencia 2026 se tiene proyectado realizar una mejora a los controles del SGSI que se encuentran en la actualidad en un estado administrado o u optimizado. Esto con el fin de fortalecer el SGSI. Para los controles que se encuentran en una etapa inicial, limitado o definido se realizará una priorización para lograr implementar, operar y mejorar estos controles y así poder contribuir a la mejora continua de estos controles los cuales son necesarios para proteger los activos de información y reducir los riesgos identificados en el INM.

d. Gestión de Incidentes y Continuidad de la Seguridad de la Información

Este eje tiene como finalidad la de fortalecer la capacidad institucional para prevenir, detectar, responder y recuperarse oportunamente frente a incidentes de seguridad de la información, minimizando impactos operativos, legales y reputacionales para el INM.

e. Uso, Apropiación y Cultura de Seguridad de la Información

Uno de los pilares y estrategias para la vigencia 2026 es la de lograr una consolidación de la cultura organizacional orientada a la protección de la información, promoviendo la responsabilidad individual, la apropiación del MSPI y la adopción de comportamientos seguros por parte de servidores públicos,

contratistas y terceros. Esto desde una visión de correspondencia frente al rol que ocupan en la entidad, su responsabilidad frente a los activos de información y la gestión que se ejecuta desde cada proceso.

f. Monitoreo, Evaluación y Mejora Continua del MSPI

Este eje tiene el objetivo de evaluar de manera sistemática el desempeño del Sistema de Seguridad y Privacidad de la Información y asegurar su mejora continua, mediante la medición de indicadores, la ejecución de una auditoría y las revisiones periódicas por parte de la Oficial de Seguridad de la información y la ejecución de revisión por la Dirección desde la OAP.

g. Tratamiento de Datos Personales

Este eje tiene el objetivo de dar cumplimiento al decreto ley 1581 de 2013 con la implementación de los lineamientos de protección de datos personales en el INM.

9. ACTIVIDADES Y CRONOGRAMA:

Se han definido unas actividades programadas para cada eje; esto con el fin de lograr posicionar el SGSI a nivel estratégico u táctico y a su vez contribuir en su implementación y mejoramiento continuo en la vigencia 2024-2026. Para poder visibilizar las actividades se cuenta con el PLAN ANUAL DEL SGSI y el Plan de Implementación de Datos personales, el cual se adjunta al presente documento.

10. ASIGNACIÓN PRESUPUESTAL PARA LA VIGENCIA 2026

Se han asignado recursos para garantizar la eficacia del SGSI y el MSPI, los cuales se relacionan a continuación:

AÑO 2026		
Ítem	**Proyecto**	**Inversión**
1	Implementación de backups fuera de sitio	$94.281.134
2	Soporte NAC, SIEM, inteligencia de amenazas y SOC	$575.647.349
3	Servicio de Ethical hacking	$ 20.125. 000

AÑO 2026		
Ítem	**Proyecto**	**Inversión**
4	Servicios profesionales para articular en el sistema integrado de gestión (SIG) el sistema de gestión de seguridad y privacidad de la información,	$ 84.588.504
Total		**$ 754.516.987**

11. ANEXOS

- Plan Anual SGSI
- Plan de Implementación de Datos Personales
- Plan de Tratamiento de Riesgos de Seguridad de la Información

12. RESPONSABLES:

El presente Plan establece de manera clara los roles y responsabilidades de las instancias y actores involucrados en su aprobación, provisión de recursos, implementación y seguimiento, con el fin de asegurar una ejecución articulada, eficiente y alineada con los objetivos institucionales. En este marco, el Comité Institucional de Gestión y Desempeño (CIGD) es la instancia encargada de aprobar el Plan; el Jefe de la OIDT debe garantizar la disponibilidad de los recursos necesarios y velar por la implementación de la plataforma tecnológica definida; el equipo de la OIDT es responsable de ejecutar dicha implementación; el CISO tiene a su cargo supervisar la correcta puesta en marcha del Plan; y el responsable de seguridad de la información coordina las actividades requeridas para su implementación integral y oportuna.

_____

Alejandra Villabón Aldana
Responsable SGSI.
Fecha: 2026-01- 21