



Departamento Nacional de Planeación



PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OFICINA DE TECNOLOGÍA Y SISTEMAS DE LA INFORMACIÓN

DEPARTAMENTO NACIONAL DE PLANEACIÓN

2026

Contenido

1.	OBJETIVOS	3
1.1.	Objetivo General	3
1.2.	Objetivos Específicos.....	3
2.	ALCANCE	3
3.	DOCUMENTOS DE REFERENCIA Y GLOSARIO	4
4.	GLOSARIO.....	4
5.	ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	5
5.1.	Resultados Instrumentos de medición	5
5.1.1.	Indicadores partes interesadas	5
6.	ESTRATEGIA DE SEGURIDAD DIGITAL	6
6.1.	Descripción de las estrategias específicas (ejes)	6
6.2.	Actividades.....	7
6.3.	Alineación con los objetivos del componente de seguridad de la información.....	8
7.	ANÁLISIS PRESUPUESTAL.....	9
8.	CONTROL DE VERSIONES	9

1. OBJETIVOS

1.1. Objetivo General

Realizar el mejoramiento continuo del componente de gestión de seguridad de la información en el DNP, con fin de mitigar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información digital institucional, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para la vigencia 2026.

1.2. Objetivos Específicos

- Fortalecer la cultura de seguridad de la información en la Entidad a través de la ejecución integral del Plan de capacitación, sensibilización y comunicación de seguridad de la información alineado con el Plan institucional de Capacitación PIC.
- Mejorar la protección y gestión de los activos de información del DNP mediante la actualización periódica de los activos de información y la declaración de aplicabilidad ISO 27001.
- Evaluar y mitigar riesgos de seguridad de la información mediante la realización de ejercicios de ingeniería social, el monitoreo de primera y segunda línea de defensa y la actualización del autodiagnóstico del Anexo 3 de Seguridad Digital de la Resolución 1519 de 2019.
- Actualizar el autodiagnóstico Modelo de seguridad y Privacidad de la información (MSPI), el autodiagnóstico de la Resolución 500 de 2021 y el autodiagnóstico Resolución 746 de 2022.

2. ALCANCE

El Plan Estratégico de Seguridad de la Información al buscar la mejora continua el componente de Gestión de Seguridad de la Información y la estrategia de seguridad digital del DNP, comparte el alcance definido dentro M-PG-07 Manual Operativo de Seguridad de la información y el MC Manual del SIG, donde se indica que el componente de seguridad aplica a todos los procesos de la Entidad incluidos en el Modelo de Operación por procesos.

3. DOCUMENTOS DE REFERENCIA Y GLOSARIO

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para la definición de actividades:

- Decreto 612 de 2018. *“Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”*, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Resolución 1519 de 2019 Anexo 3. *“Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”*
- Resolución 500 de 2021. *“Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”*.
- Resolución 2277 de 2025. *“Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia”*
- Resolución 746 de 2022. *“Por la cual se fortalece el modelo de seguridad y privacidad de la información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021”*
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC
- Anexo 1 - Normograma y otros documentos de origen externo que contiene la normativa relacionada con seguridad de la información.
- Índice de Gobierno Digital
- Medición del Desempeño Institucional (Política Seguridad Digital)
- Medición del Desempeño Institucional (Política Seguridad Digital)
- Normas ISO de Seguridad de la información ISO 27001:2013 , ISO 27002:2015, ISO 27001:2022 ISO 27002:2022.
- Informes de auditorías de control interno del Departamento Nacional de Planeación.
- M-PG-07 Manual Operativo de Seguridad de la Información
- M-PG-12 Manual para la política de tratamiento de la información de datos personales
- M-PG-16 Manual Gestión Integral de Riesgos
- PT-PG-01 Procedimiento Gestión integral de riesgos
- PT-TI-01 Procedimiento Atención a Requerimientos de Servicios TIC que incluye la de gestión de incidentes.

4. GLOSARIO

- Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas
- Seguridad de la Información: Este principio de la Política de Gobierno Digital busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.
- Seguridad digital: Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital (ii) la implementación efectiva de medidas de ciberseguridad y (iii) el uso efectivo de las capacidades de ciberdefensa que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

- Seguridad Informática: o también llamada ciberseguridad, se refiere a la protección de la información y, especialmente, al procesamiento que se hace de la misma, con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas. Su principal finalidad es que tanto personas como equipos tecnológicos y datos estén protegidos contra daños y amenazas hechas por terceros.

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

Los siguientes datos demuestran la mejora continua y el compromiso de la Entidad por la implementación de controles y lineamientos en seguridad de la información, seguridad informática y seguridad digital acorde a los lineamientos del Gobierno Nacional.

5.1. Resultados Instrumentos de medición

5.1.1. Indicadores partes interesadas

Como Entidad del Gobierno Nacional, el DNP evalúa el cumplimiento de las políticas de Gobierno Digital y Seguridad Digital a través diferentes instrumentos. La siguiente tabla presenta el porcentaje obtenido en el año 2025.

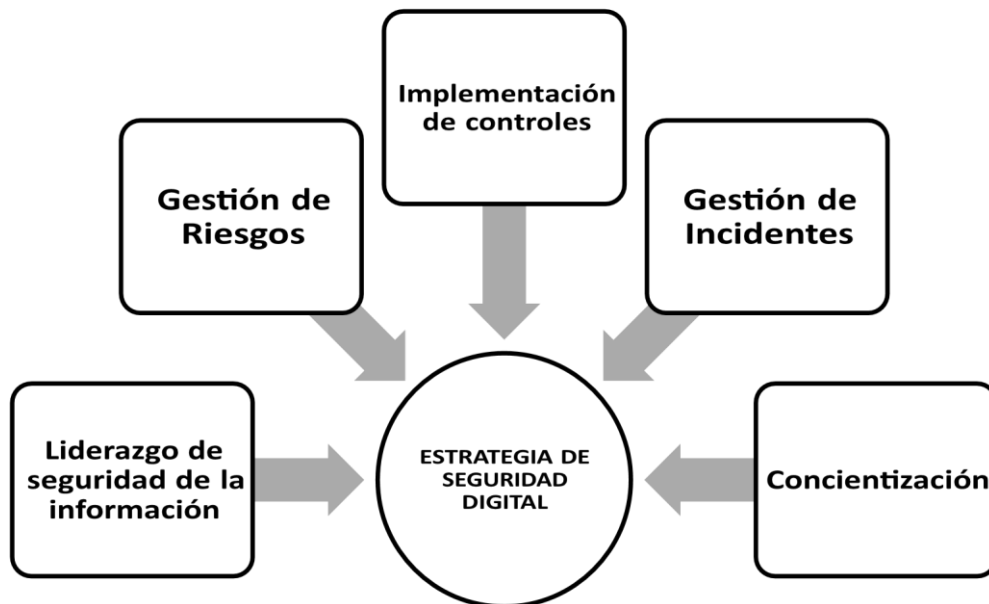
Nombre del indicador	Descripción	Porcentaje 2025
MSPi MINTIC (ISO 27001:2022)	Resultado del autodiagnóstico del Modelo de privacidad y seguridad de la información (instrumento MINTIC)	81%
FURAG 2024	Resultado de la evaluación de la política de seguridad digital la información es recolectada en el FURAG	92%
Índice Gobierno Digital 2024	Resultado de la evaluación del Habilitador de Seguridad y Privacidad de la Información la información es recolectada en el FURAG	83,4%
Resolución 746 de 2022	Resultado del autodiagnóstico del Modelo de privacidad y seguridad de la información (instrumento MINTIC)	76%
RNBD	Cantidad de registro de bases de datos personales actualizados y nuevos en el aplicativo de la Superintendencia de industria y Comercio	103
Incidentes datos personales	Cantidad de incidentes de seguridad reportados en el aplicativo de la Superintendencia de industria y Comercio	0
Incidentes reportados al Colcert	Se gestionaron 9 incidentes menores. Los incidentes menores están relacionados con a) afinamiento de las reglas de correo electrónico para identificar correos maliciosos, b) Conato de incendio c) Reporte de detección de credenciales expuestas en fuentes abiertas.	9

La herramienta que permite el cumplimiento de los porcentajes es el Plan especial de gestión de seguridad y privacidad de la información asociado al Plan de Acción.

6. ESTRATEGIA DE SEGURIDAD DIGITAL

En cumplimiento de la Resolución 500 de 2021 y Resolución 2277 de 2025, la Entidad establece una estrategia de seguridad digital 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 se basa en la implementación del Modelo de Seguridad y Privacidad de la Información MSPi de MINTIC, los manuales y procedimientos institucionales .

Por tal motivo, el DNP define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



Fuente: MINTIC https://gobiernodigital.mintic.gov.co/692/articles-401785_recurso_1.docx

6.1. Descripción de las estrategias específicas (ejes)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI, la Resolución 500 de 2021 y la Resolución 2277 de 2025:

ESTRATEGIA/EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPi) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados teniendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.

ESTRATEGIA/EJE	DESCRIPCIÓN/OBJETIVO
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

6.2. Actividades

Las estrategias se gestionan con el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información solicitados por el Decreto 612 de 2018, los cuales están incluidos en el Plan de Acción Institucional del DNP del año 2026 así:

Proceso	PLANEACIÓN Y GESTIÓN ORIENTADA A RESULTADOS	PLANEACIÓN Y GESTIÓN ORIENTADA A RESULTADOS
Nombre Línea Acción	Administración y mantenimiento del MOP	Administración y mantenimiento del MOP
Nombre Procedimiento	Planeación y mantenimiento del MOP	Planeación y mantenimiento del MOP
Código Producto	7216	7437
Nombre Producto	Informes plan especial de gestión de seguridad y privacidad de la información entregado	Informe de las actividades realizadas para la identificación y clasificación de activos de información entregado
Código Entregable	22784	24253
Nombre Entregable	Informes plan especial de gestión de seguridad y privacidad de la información entregado	Informe de las actividades realizadas para la identificación y clasificación de activos de información entregado
Denominación Entregable	Informes plan especial de gestión de seguridad y privacidad de la información entregado	Informe de las actividades realizadas para la identificación y clasificación de activos de información entregado
Fecha Fin	31/dic/2026	31/dic/2026
Fecha Inicio	1/ene/2026	1/ene/2026

6.3. Alineación con los objetivos del componente de seguridad de la información

Las actividades definidas están alineadas a los cuatro objetivos específicos del componente de seguridad de la información

Plan	Objetivo CGSI	Estrategia	Actividad
Plan de Seguridad y Privacidad de la Información	OECS2: Fortalecer la adopción del Modelo de seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el componente de seguridad de la Información	Liderazgo de seguridad de la información	Estructurar los planes de seguridad de acuerdo con el Decreto 612 de 2018
Plan de Seguridad y Privacidad de la Información	OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.	Implementación de controles	Actualizar los documentos del componente de seguridad de la información
Plan de Seguridad y Privacidad de la Información	OECS2: Fortalecer la adopción del Modelo de seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	Actualizar los activos de información
Plan de Seguridad y Privacidad de la Información	OECS3: Crear una cultura de seguridad de la información, como medida preventiva para mitigar los riesgos que afecten la información digital y ofrecer un lenguaje común sobre de seguridad de la información dentro de la Entidad.	Concientización	Actualizar y ejecutar el plan de capacitación, sensibilización y comunicación de seguridad de la información
Plan de Seguridad y Privacidad de la Información	OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Gestión de incidentes	Realizar el reporte de los Indicadores de seguridad de la información
Plan de Seguridad y Privacidad de la Información	OECS3: Crear una cultura de seguridad de la información, como medida preventiva para mitigar los riesgos que afecten la información digital y ofrecer un lenguaje común sobre de seguridad de la información dentro de la Entidad.	Implementación de controles	Realizar el seguimiento a la implementación de Directiva Presidencial 1 de 2024 (Ahorro Energía)
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	OECS3: Crear una cultura de seguridad de la información, como medida preventiva para mitigar los riesgos que afecten la información digital y ofrecer un lenguaje común sobre de seguridad de la información dentro de la Entidad.	Implementación de controles	Actualizar controles de seguridad de la información
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Implementación de controles	Monitoreo de riesgos de seguridad de la información

7. ANÁLISIS PRESUPUESTAL

Las adquisiciones de seguridad de la información que se requieran se gestionan a través del plan anual de adquisiciones disponible en <https://www.dnp.gov.co/LaEntidad/secretaria-general/Subdireccion-contratacion/contratacion/Paginas/plan-anual-de-adquisiciones.aspx>, y el proyecto de inversión “Fortalecimiento de las tic para el cumplimiento de los objetivos del DNP a nivel Nacional”.

8. CONTROL DE VERSIONES

Los planes de tratamiento de riesgos de seguridad y privacidad de la información, así como el plan de seguridad y privacidad de la información en los que se basa este documento, fueron presentados para la consideración y revisión de la alta dirección y el comité de gestión y desempeño institucional, con el objetivo de ser aprobados y aplicados de acuerdo con lo aquí establecido.

Elaboró:

Sandra Fernanda Poveda Oficial de Seguridad de la información.
18 de enero de 2026

Revisó:

Orlando Benavides Santacruz
Jefe Oficina de Tecnología y sistemas de la información
19 de enero de 2026

Oficina Asesora de planeación

Soporte: Solicitud de integración de los planes institucionales-Decreto 612 de 2018 enviado a Sistema Gestion de Calidad
gpcalidad@dnp.gov.co
22 de enero de 2026

Aprobó:

Comité institucional de Gestión y Desempeño
29 enero 2026