PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2024-2026

Superintendencia Nacional de Salud

Área Responsable: Subdirección de Tecnologías de la información

(versión 2)

2026 – Enero

Supersalud

Bernardo Armando Camacho Rodríguez - **Superintendente Nacional de Salud**

Rainer Narval Naranjo Charrasquiel - **Secretaría General**

Genaro Ballén Hernández - **Delegatura de Investigaciones Administrativas**

Gustavo Adolfo Flechas Ramírez - **Delegatura para la Función Jurisdiccional y de** Conciliación

María Niny Echeverry Prada - **Delegatura para la Protección al Usuario**

María Yuleidy López Ramírez - **Delegatura para Entidades de Aseguramiento en Salud**

Edilma Marlen Suarez Castro - **Delegatura para Entidades Territoriales y Generadores, Recaudadores y administradores de Recursos del SGSSS**

Beatriz Eugenia Gómez Consuegra - **Delegatura para Prestadores de Servicios en Salud**

Mónica Patricia Almonacid Guzmán - **Delegatura para Operadores Logísticos de Tecnologías en Salud y Gestores Farmacéuticos**

Gloria Rocío Pereira Oviedo - **Jefe Oficina Asesora de Planeación**

Jazmín Maritza La Rotta Bernal - **Jefe Oficina Asesora de Comunicaciones Estratégicas e Imagen Institucional**

Gressy Kareny Rojas Cardona-**Dirección Jurídica**

Juan Sebastián Emanuel Sierra Álvarez - **Oficina de Liquidaciones**

José Alexander de los Reyes Aldana - **Dirección de Innovación y Desarrollo**

Giovanny López Mejia-**Oficina de Control Interno**

Contenido

1. Plan de Seguridad y Privacidad de la Información

Introducción

La Superintendencia Nacional de Salud reconoce la información como uno de los activos más importantes y críticos para el cumplimiento de sus funciones misionales. En el desarrollo de las actividades de sus procesos se gestiona, almacena, custodia, transfiere e intercambiar información valiosa que no debe ser divulgada a personal no autorizado, situación que podría poner en riesgo la gestión pública. La protección de los activos de información constituye una labor esencial para garantizar la continuidad institucional, el logro de los objetivos estratégicos y el cumplimiento del marco normativo aplicable, al tiempo que fortalece la confianza de las partes interesadas.

En atención a lo anterior, y en concordancia con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), la Superintendencia Nacional de Salud establece el Plan de Acción de Seguridad y Privacidad de la Información 2026, el cual define la hoja de ruta de la estrategia de seguridad digital orientada a gestionar y proteger la información suministrada a la Entidad y la generada por esta, frente a las diversas amenazas que puedan afectar su integridad, disponibilidad, confidencialidad y privacidad.

Este plan contempla la planeación de actividades que contribuyan a la mejora continua del Sistema de Gestión de Seguridad Digital (SGSD) y del Programa Integral de Protección de Datos Personales, incorporando las propuestas y oportunidades de mejora identificadas durante la gestión del año 2025. Así mismo, se articula con el Plan de Acción de Tratamiento de Riesgos de Seguridad y se

desarrolla conforme a los lineamientos del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones.

Información general

Nombre del Plan de acción o estrategia institucional	Plan de Seguridad y Privacidad de la Información
Nombre y código rubro presupuestal asociado	
Presupuesto asignado ($)	
Área responsable	Subdirección de Tecnologías de la Información
Política asociada y otros lineamientos	8. Seguridad digital
Proceso	Gestión de Tecnologías de la Información
Fecha de inicio	02/01/2026
Fecha de finalización	31/12/2026

1. propósito del plan

Objetivo Estratégico

Optimizar los procesos a través del mejoramiento tecnológico, de la cultura organizacional y del gobierno corporativo para atender las necesidades de los grupos de incidencia.

Objetivo General

Definir las actividades y los roles necesarios para la implementación del Modelo de Seguridad y Privacidad de la Información en la vigencia 2026, en cumplimiento de la metodología establecida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y el Departamento Administrativo de la Función Pública. El propósito es proteger, preservar y gestionar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información, favoreciendo la optimización de los procesos institucionales a través del mejoramiento tecnológico, la consolidación de la cultura organizacional y el fortalecimiento del gobierno corporativo, para atender oportunamente las necesidades de los grupos de interés de la entidad.

Objetivos Específicos

Planificar, ejecutar y hacer seguimiento a las actividades que integran el Sistema de Gestión de Seguridad Digital durante la vigencia 2026, conforme a los lineamientos institucionales y normativos.

Desarrollar, actualizar y mantener el Programa Integral de Protección de Datos Personales para garantizar la adecuada gestión y protección de la información personal en poder de la entidad.

Implementar las oportunidades de mejora identificadas en el Sistema de Gestión de Seguridad Digital a partir de los resultados y hallazgos de la gestión realizada en la vigencia 2025, promoviendo la mejora continua y la adaptación a nuevas amenazas y requerimientos.

Alcance

El Plan de Seguridad y Privacidad de la Información incluye las actividades exigidas por la normativa vigente, así como la atención a las necesidades de las áreas en materia de seguridad y privacidad, en coherencia con el Modelo de Seguridad y Privacidad de la Información, la Política de Seguridad Digital y el Programa Integral de Protección de Datos Personales.

Normatividad

El presente normograma compila y organiza el marco normativo vigente y aplicable que fundamenta la gestión de la seguridad y privacidad de la información en la Entidad. Este instrumento orientador relaciona las leyes, decretos, resoluciones, circulares, documentos CONPES, lineamientos técnicos y directivas institucionales que establecen los principios, obligaciones y mejores prácticas para la protección de los activos de información, el tratamiento adecuado de datos personales y la gestión integral de riesgos digitales.

Leyes

Ley 1581 de 2012 – Protección de Datos Personales (y proyecto de actualización en trámite 2025)

Ley 1712 de 2014 – Transparencia y Derecho de Acceso a la Información Pública

Ley 2088 de 2021 – Régimen del Trabajo en Casa

Ley 1266 de 2008 – Habeas Data financiero

Decretos

Decreto 1074 de 2015 – Único Reglamentario del Sector Comercio, Industria y Turismo (registro bases de datos)

Decreto 1078 de 2015 – Único Reglamentario del Sector TIC

Decreto 1083 de 2015 – Único Reglamentario de Función Pública

Decreto 1377 de 2013 – Reglamenta parcialmente la Ley 1581 de 2012

Decreto 338 de 2022 – Lineamientos para fortalecimiento de gobernanza en seguridad digital

Decreto 2106 de 2019 – Estrategia de seguridad digital

Decreto 612 de 2018 – Integración de planes institucionales y estratégicos

Resoluciones y Circulares (MinTIC, SIC y Supersalud)

Resolución 500 de 2021 – Lineamientos y estándares para la estrategia de seguridad digital/MSPI

Resolución 460 de 2022 – Plan Nacional de Infraestructura de Datos

Resolución 1519 de 2020 – Estándares para publicar información (acceso, seguridad, datos abiertos)

Resolución 1321 de 2020 – Parámetros mínimos para gestión de riesgos tecnológicos (sector salud)

Circular Externa 002 de 2024 (SIC) – Tratamiento de datos personales en sistemas de IA

Circular Externa 001 de 2025 (SIC) – Medidas de seguridad de la información y reporte de incidentes

Circulares Superintendencia Financiera 029 de 2014 y 033 de 2020 – Riesgo ciberseguridad, reporte de incidentes.

Resolución 02277 de 2025 - Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.

Lineamientos Técnicos y Modelos

Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC, actualizado 2025

Norma Técnica Colombiana NTC-ISO/IEC 27001:2022 – Gestión de Seguridad de la Información

Modelo Integrado de Planeación y Gestión (MIPG) – Dimensión Seguridad Digital

Guía DAFP: Administración del Riesgo y Diseño de Controles

CONPES y Políticas Nacionales

CONPES 3701 de 2011 – Estrategia Nacional Ciberseguridad y Ciberdefensa

CONPES 3854 de 2016 – Política Nacional de Seguridad Digital

CONPES 3995 de 2020 – Política Nacional de Confianza y Seguridad Digital

Directivas Presidenciales

Directiva Presidencial 03 de 2021 – Lineamientos para uso de nube, IA y seguridad digital

Directiva Presidencial 02 de 2022 – Estrategia para actualización, gestión integral y seguridad digital

2. Marco estratégico

Formulación del plan de acción o estrategia institucional

2.1. Generalidades del plan de acción o estrategia institucional

El Plan de Seguridad y Privacidad de la Información 2026 se formula en coherencia con el objetivo estratégico institucional orientado a optimizar los procesos a través del mejoramiento tecnológico, de la cultura organizacional y del gobierno corporativo para atender las necesidades de los grupos de incidencia. En este marco, el Plan busca fortalecer el Sistema de Gestión de Seguridad y Privacidad de la Información de la Superintendencia Nacional de Salud como un componente esencial para la eficiencia institucional, la confianza digital y la consolidación de una cultura organizacional responsable en el tratamiento y protección de la información.

Su formulación parte de un análisis comparativo entre la situación actual y la situación deseada del Sistema de Gestión de Seguridad y Privacidad de la Información, con el propósito de identificar brechas, priorizar acciones y establecer estrategias orientadas a alcanzar un mayor nivel de madurez en la gestión de la seguridad y la privacidad de la información. Este enfoque garantiza la alineación con las políticas nacionales, los estándares internacionales (ISO 27001:2022) y los

lineamientos definidos por la Alta Dirección de la Superintendencia Nacional de Salud.

3. Diagnóstico de la situación

3.1. Situación actual

La Superintendencia Nacional de Salud cuenta con un Sistema de Gestión de Seguridad Digital estructurado y en implementación continua, respaldado por políticas, procedimientos y controles alineados con la norma ISO 27001:2022. Los resultados del Formulario Único de Reporte de Avances de la Gestión (FURAG) 2024, con un puntaje de 86% en la Política de Seguridad Digital, demuestran el compromiso institucional con la gestión de riesgos tecnológicos, la mejora continua y la protección de los activos de información.

En este contexto, la Subdirección de Tecnologías de la Información ejerce actualmente la función de liderar la gobernanza de la seguridad de la información dentro de la Superintendencia Nacional de Salud. Esta dependencia ha asumido la coordinación y el monitoreo integral de las acciones vinculadas con la gestión del riesgo digital y el cumplimiento de los controles de seguridad, promoviendo una visión unificada de la gestión de la seguridad al interior de la entidad. Sin embargo, se ha identificado la necesidad de fortalecer su articulación técnica con las demás dependencias operativas y misionales, con el fin de lograr una implementación más efectiva y homogénea del Sistema de Gestión de Seguridad Digital y del Programa Integral de Protección de Datos Personales.

De igual manera, las pruebas de controles y revisiones internas han evidenciado oportunidades de mejora en la efectividad de algunos controles relacionados con la administración de vulnerabilidades, la trazabilidad de acciones correctivas y la

actualización continua frente a las nuevas amenazas tecnológicas. Estos retos reflejan la importancia de consolidar un enfoque de seguridad integral y preventivo que abarque tanto los aspectos tecnológicos como los organizacionales.

4. Estrategias

4.1. Situación deseada

Para el año 2026, la Superintendencia Nacional de Salud proyecta un Sistema de Gestión de Seguridad y Privacidad de la Información maduro, ágil y completamente integrado con la planeación estratégica institucional. Este sistema debe garantizar la incorporación de medidas de seguridad y privacidad en los procesos, proyectos y servicios de la entidad, contribuyendo al fortalecimiento de la confianza ciudadana y al cumplimiento de los marcos normativos en materia de seguridad digital y protección de datos.

La Subdirección de Tecnología, como área encargada de liderar la gobernanza de la seguridad de la información, articulará sus acciones con todas las dependencias de la Superintendencia Nacional de Salud, asegurando la coherencia y efectividad de las políticas y controles definidos. Este rol integrador permitirá fortalecer la gestión institucional del riesgo digital, optimizar la protección de los datos personales y promover la mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información a partir de un trabajo colaborativo y coordinado con las áreas de tecnología, jurídica, planeación, talento humano y demás instancias que intervienen en la cadena de valor institucional.

En este marco, el Plan para la vigencia 2026 establece los siguientes ejes estratégicos:

Fortalecer la infraestructura y las capacidades de monitoreo, detección y respuesta ante incidentes, consolidando la operación del SOC/CSIRT y mejorando los tiempos de reacción ante eventos de seguridad.

Integrar la gestión del riesgo de seguridad y privacidad al ciclo de planeación institucional y al diseño de servicios digitales, garantizando una protección preventiva y sostenible.

Fomentar una cultura organizacional orientada a la seguridad de la información mediante procesos de sensibilización, capacitación y corresponsabilidad institucional.

Potenciar la gobernanza de la seguridad digital y la eficacia del Sistema de Gestión de Seguridad y Privacidad de la Información a través del seguimiento permanente de las auditorías, la trazabilidad de los controles y la mejora continua de los procesos.

Consolidar la protección de los datos personales conforme con los principios de privacidad desde el diseño y por defecto, basados en el cumplimiento del Programa Integral de Protección de Datos Personales.

La ejecución de este Plan permitirá fortalecer la gestión tecnológica y la gobernanza de la seguridad de la información en la Superintendencia Nacional de Salud, consolidando un modelo institucional más seguro, resiliente y orientado a la excelencia operativa en beneficio de sus grupos de incidencia.

5. Cronograma

El cronograma se presenta como adjunto en el formato DEFT35 dentro del mismo se relacional las actividades del Plan de Acción de Seguridad y Privacidad de la Información para el año 2026:

6. Seguimiento y evaluación

Con el fin de garantizar un seguimiento y evaluación al plan de acción, se establece los siguientes indicadores:

Porcentaje de participación en inducciones, reinducciones y/o sensibilizaciones en Seguridad Digital

Fórmula:

$$= \left(\frac{\text{Número de colaboradores que participaron en inducciones, reinducciones o sensibilizaciones}}{\text{Número total de empleados}}\right) \times 100$$

Fuente: registros de capacitación anual

Periodicidad: anual

Meta: 70%

Porcentaje de Cumplimiento Plan de Acción

Fórmula:

$$= \left(\frac{\text{Número de actividades del Plan de Acción realizadas en el trimestre}}{\text{Número total de actividades planificadas en el trimestre}}\right) \times 100$$

.

Fuente: informes trimestrales del plan de trabajo

Periodicidad: trimestral

Meta: 95%