

	PROCESO GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN	CÓDIGO	DIP105
	POLÍTICA DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN	VERSIÓN	1
		FECHA	21/10/2025

En un entorno institucional cada vez más digitalizado y expuesto a riesgos cibernéticos, la Superintendencia Nacional de Salud (SNS), como entidad encargada de la inspección, vigilancia y control del Sistema General de Seguridad Social en Salud (SGSSS), enfrenta el reto de proteger grandes volúmenes de información crítica, incluyendo datos personales de salud, financieros y operativos.

Según el informe de ciberseguridad del sector salud 2024, el 73% de las entidades del sector han experimentado al menos un incidente de seguridad en los últimos dos años, siendo el ransomware y el acceso no autorizado a datos personales las principales amenazas. La creciente sofisticación de los ciberataques, sumada a la sensibilidad de la información tratada por la SNS, ha evidenciado la necesidad de establecer un marco institucional claro que oriente la actuación de los funcionarios y contratistas frente a situaciones que comprometan la seguridad digital y la seguridad de la información en la operación de la entidad.

Esta situación representa una oportunidad para consolidar un enfoque institucional basado en la gestión del riesgo, la mejora continua y la corresponsabilidad, en cumplimiento del Decreto 1078 de 2015, la Ley 1581 de 2012, la Ley 1273 de 2009, el Documento CONPES 3995 de 2020, el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, las normas ISO/IEC 27001 y 27002, el Marco de Ciberseguridad del NIST y las guías de la SIC sobre protección de datos personales.

	PROCESO GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN	CÓDIGO	DIP105
	POLÍTICA DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN	VERSIÓN	1
		FECHA	21/10/2025

Declaratoria

La Superintendencia Nacional de Salud se compromete a implementar, fortalecer y mantener su Seguridad Digital y Seguridad de la Información mediante un enfoque integral que garantice la confidencialidad, integridad y disponibilidad de la información institucional, articulando un marco normativo, técnico y operativo que promueva la gestión responsable y proactiva de los riesgos de Seguridad Digital, adoptando controles organizacionales y tecnológicos, fomentando una cultura de seguridad en toda la entidad a través de la capacitación a su talento humano.

Este compromiso se materializa en la adopción de lineamientos claros y obligatorios que orienten el comportamiento de todos los actores institucionales frente al uso, tratamiento y protección de la información; que permita prevenir, detectar, responder y recuperar ante eventos que comprometan la seguridad digital y la integridad de la información institucional.

La política institucional será implementada mediante acciones concretas de sensibilización, control, monitoreo y evaluación, con el respaldo de la alta dirección y en articulación con los procesos estratégicos, misionales y de apoyo de la entidad.

Para materializar este compromiso institucional, la Superintendencia Nacional de Salud establece las siguientes directrices que orientarán la implementación de la política:

	PROCESO GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN	CÓDIGO	DIP105
	POLÍTICA DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN	VERSIÓN	1
		FECHA	21/10/2025

Directriz	Objetivo	Indicador
Implementar un Sistema de Gestión de Seguridad de la Información alineado con estándares internacionales y normatividad nacional, que incluya gobierno de seguridad, gestión de riesgos, controles técnicos y organizacionales, gestión de incidentes y capacitación continua	Fortalecer la postura de ciberseguridad y protección de la información de la Superintendencia Nacional de Salud para salvaguardar la información sensible y crítica, asegurando la continuidad de sus operaciones y la confianza de los ciudadanos	• Reducción porcentual de incidentes de seguridad críticos y altos. • Porcentaje de cumplimiento de controles de seguridad en sistemas críticos. • Tiempo promedio de respuesta ante incidentes reportados. Plan de Seguridad y Privacidad de la información.
Establecer controles de acceso, cifrado de información, protección contra amenazas, copias de seguridad y monitoreo continuo de	Proteger los activos de información mediante la implementación de salvaguardas técnicas que reduzcan la	• Porcentaje de sistemas con controles de acceso implementados (Meta: 100% -

	PROCESO GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN	CÓDIGO	DIP105
	POLÍTICA DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN	VERSIÓN	1
		FECHA	21/10/2025

Directriz	Objetivo	Indicador
la infraestructura tecnológica	exposición a riesgos cibernéticos	Medición mensual • Numero de amenazas identificadas. Mapa de riesgos de seguridad de la información. Reporte de amenazas identificadas mediante herramienta de seguridad perimetral.
Gestionar capacitaciones y sensibilizaciones en seguridad de la información dirigido a funcionarios, contratistas y terceros	Crear una cultura organizacional de seguridad que fortalezca el factor humano como primera línea de defensa ante amenazas cibernéticas	• Porcentaje de funcionarios capacitados en seguridad de la información. • Numero de capacitaciones y sensibilizaciones por semestre.

	PROCESO GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN	CÓDIGO	DIP105
	POLÍTICA DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN	VERSIÓN	1
		FECHA	21/10/2025

Directriz	Objetivo	Indicador
		Resultados del índice de Desempeño Institucional (IDI).

Esta política tiene alcance para la totalidad de la información institucional que se gestiona en el marco de los procesos de la entidad, aplicando a todos los funcionarios, contratistas, terceros, procesos y sedes donde opere directamente la Superintendencia Nacional de Salud, así como las áreas tercerizadas u otras instancias que afecten la prestación del servicio.

Incluye la información que se genera, recibe, procesa, almacena, transmite o elimina en el ejercicio de las funciones institucionales, que es utilizada por funcionarios, contratistas, terceros o exfuncionarios durante su vinculación con la entidad, que circula en medios físicos o digitales, sin importar su nivel de clasificación o sensibilidad, y que es utilizada durante la vinculación con la entidad.

Por tanto, las políticas establecidas son de aplicación obligatoria para funcionarios, contratistas, procesos y sedes, así como los servicios tercerizados y demás instancias que impacten la prestación del servicio.

El despliegue de la política estará a cargo de la alta dirección en cabeza de la Subdirección de Tecnologías de la Información como líder de la implementación del Sistema de Gestión de Seguridad de la Información, con

	PROCESO GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN	CÓDIGO	DIP105
	POLÍTICA DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN	VERSIÓN	1
		FECHA	21/10/2025

la coordinación del Oficial de Seguridad (CISO), el apoyo del grupo de seguridad digital y el compromiso de todos los funcionarios de la entidad.

El equipo directivo de la entidad, incluyendo directores, subdirectores y jefes de oficina, tiene la responsabilidad de garantizar el cumplimiento de la política en sus dependencias, mientras que todos los funcionarios, contratistas y terceros que interactúan con la información institucional son corresponsables de su adecuada protección y del cumplimiento de los lineamientos establecidos.

La implementación de la presente política se desarrollará como un proceso continuo y sistemático, que iniciará con la identificación y análisis de riesgos sobre los activos de información, con el propósito de priorizar controles y definir medidas de mitigación efectivas. Estos controles se establecerán desde una perspectiva técnica, administrativa y física, y se integrarán en políticas operativas que serán documentadas y actualizadas en los manuales correspondientes, garantizando así su correcta aplicación.

De manera complementaria, se promoverá una cultura organizacional de seguridad mediante procesos de capacitación continua dirigidos a funcionarios, contratistas y terceros, con el fin de cerrar brechas de desempeño y fortalecer la gestión de la seguridad en el sector. Asimismo, se desarrollarán auditorías internas periódicas para verificar el cumplimiento de esta política y de los procedimientos asociados. Finalmente, todas las acciones estarán alineadas con la legislación nacional vigente, incluyendo las normas sobre protección de datos personales, delitos informáticos y derechos de autor.

 Supersalud 	PROCESO GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN		CÓDIGO	DIP105
	POLÍTICA DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN		VERSIÓN	1
			FECHA	21/10/2025

Registro de aprobación					
Elaboró		Revisó		Aprobó	
Nombre	Julio Cesar Mancipe Caicedo	Nombre	Diego Hernando Sierra Millan Julio Cesar Mancipe Caicedo	Nombre	Yasmin Marín Gomez
Cargo	Asesor de Despacho Oficial de Seguridad CISO	Cargo	Subdirector Tecnologías de Información (e) Oficial de Seguridad CISO	Cargo	Directora Dirección de Innovación y Desarrollo
Fecha	09/07/2025	Fecha	02/10/2025	Fecha	07/10/2025