

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 1 de 25</p>

Plan de Privacidad y Seguridad de la Información
2025-2026
Versión 04

GOBIERNO DIGITAL

INSTITUTO DEPARTAMENTAL DE SALUD DE NORTE DE SANTANDER

Enero de 2025

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 2 de 25</p>

Control de Versiones

Versión	Fecha	Modificación
1.0	Sep - 2020	Elaboración del Plan
2.0	Ene - 2022	Actualización documentos de referencia
3.0	Ene - 2024	Actualización y ampliación de fechas de las actividades finales de ejecución
4.0	Ene - 2025	Actualización del plan inclusión de lineamientos de la Resolución N° 746 de 2022

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 3 de 25</p>

Tabla de contenido

1. INTRODUCCIÓN	4
2. OBJETIVO.....	5
2.1 OBJETIVOS ESPECÍFICOS.....	5
3. ALCANCE.....	6
4. DOCUMENTOS DE REFERENCIA.....	7
5. DEFINICIONES.....	8
6. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	13
7. ESTRATEGIA DE SEGURIDAD DIGITAL.....	15
7.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES).....	16
8. FASES PARA PLANEAR E INSTRUMENTAR EL MODELO	17
8.1 FASE DIAGNÓSTICO.....	17
8.2 FASE PLANIFICACIÓN	18
8.3 FASE IMPLEMENTACIÓN	19
8.4 FASE EVALUACIÓN DE DESEMPEÑO	20
8.5 FASE MEJORA CONTINUA.....	21
9. CRONOGRAMA DE ACTIVIDADES.....	22
10. RESPONSABLES.....	24
11. PLAN DE COMUNICACIÓN	25

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander <small>Instituto Departamental de Salud</small></p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 4 de 25</p>

1. INTRODUCCIÓN

La Política de Gobierno Digital establecida mediante Decreto 1008 de 2018, tiene como uno de sus habilitadores transversales, la Seguridad de la Información. Y busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información.

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en el Artículo 5° de la Resolución N° 500 de 2021 establece que los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información.

El Plan de Seguridad y Privacidad de la Información contempla la protección de la información digital, medios impresos y físicos digitales y no digitales. Así mismo, la Resolución N° 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 número 500 de 2021, determinando que se deben implementar controles de protección de la privacidad en aquellos sistemas relacionados con el tratamiento de datos personales.

La estrategia de seguridad digital debe definirse en 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 del procedimiento de gestión de incidentes de seguridad digital

La seguridad y privacidad de la información en el Instituto Departamental de Salud de Norte de Santander es fundamental para garantizar la protección de los datos ciudadanos, la continuidad de los servicios y el cumplimiento de la normativa vigente en Colombia. Este plan establece las estrategias y medidas necesarias para planear y ejecutar todas las fases que permitan la adopción del MSPI y la gestión segura de la información en el periodo 2025-2026.

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 5 de 25</p>

2. OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información del Instituto Departamental de Salud de Norte de Santander, para reducir los riesgos a los que está expuesta la entidad hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2025-2026.

2.1 OBJETIVOS ESPECÍFICOS

- Implementar controles y medidas de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información.
- Reducir riesgos asociados a ciberamenazas y accesos no autorizados.
- Sensibilizar y capacitar a los funcionarios sobre buenas prácticas de seguridad de la información.
- Asegurar el cumplimiento de la normativa vigente.

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 6 de 25</p>

3. ALCANCE

El plan se aplicará a:

- Toda la infraestructura tecnológica de la entidad.
- Los datos personales y sensibles tratados por la entidad.
- Los funcionarios y contratistas con acceso a la información.
- Sistemas de información críticos, incluyendo el Observatorio de Salud Pública y la gestión de PQRS.

La ejecución de este Plan se hará con la supervisión del Comité de Gestión y Desempeño Institucional y su aplicación es responsabilidad de todos los funcionarios de planta y contratistas que laboran en el Instituto Departamental de Salud de Norte de Santander, a los cuales se les asignará competencias y responsabilidades.

El plan está formulado para que se ejecute durante la vigencia 2025 y 2026, tiempo necesario para lograr la adopción del MSPI y garantizar su continuidad.

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 7 de 25</p>

4. DOCUMENTOS DE REFERENCIA

El Plan de Seguridad y Privacidad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- 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 de Seguridad y Privacidad de la Información como uno de los requisitos a desarrollar para cumplir con esta normativa.
- 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 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 número 500 de 2021”.
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 8 de 25</p>

5. DEFINICIONES

CONCEPTO	DESCRIPCIÓN
Acceso a la Información Pública	Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
Activo	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).
Activos de información	En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
Archivo	Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
Amenazas	Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
Análisis de Riesgo	Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 9 de 25</p>

CONCEPTO	DESCRIPCIÓN
Auditoría	Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría (ISO/IEC 27000).
Autorización	Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
Bases de Datos Personales	Conjunto organizado de datos personales que sea objeto de Tratamiento (Leu 1581 de 2012, art 3)
Ciberseguridad	Capacidad del Estado para minimizar el nivel de riesgo la que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
Ciberespacio	Es el ambiente tanto físico como virtual por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
Control	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas paramantener 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.
Datos abiertos	Son todos aquellos primarios o sin procesos, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander <small>Instituto Departamental de Salud</small></p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 10 de 25</p>

CONCEPTO	DESCRIPCIÓN
Datos personales Públicos	Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión y oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva (Decreto 1377 de 2013, art 3)
Datos Personales Privados	Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
Datos personales Mixtos	Es la información que contiene datos personales públicos junto con datos privados o sensibles.
Datos Personales Sensibles	Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, a orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud a la vida sexual, y los datos biométricos (Decreto 1377 de 2013, art 3)
Encargado del Tratamiento de Datos	Persona natural o jurídica, pública o privada, que pos sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)
Gestión de incidentes de seguridad de la información	Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
Información Pública Clasificada	Es aquella información que estando en poder o custodia de una sujeta obligado en su calidad de tal, pertenece al ambiente propio, particular y privado o semiprivado de una persona natural o

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 11 de 25</p>

CONCEPTO	DESCRIPCIÓN
	<p>jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 de 2014. (Ley 1712 de 2013, art 6)</p>
<p>Información Pública Reservada</p>	<p>Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)</p>
<p>Ley de Habeas Data</p>	<p>Se refiere a la Ley Estatutaria 1266 de 2008.</p>
<p>Ley de Transparencia y Acceso a la Información Pública</p>	<p>Se refiere a la Ley Estatutaria 1712 de 2014.</p>
<p>Mecanismos de protección de datos personales</p>	<p>Lo constituye las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.</p>
<p>Plan de continuidad del negocio</p>	<p>Plan orientado a permitir a continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000)</p>
<p>Plan de tratamiento de riesgos</p>	<p>Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma (ISO/IEC 27000)</p>
<p>Privacidad</p>	<p>En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de las entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno Digital la correlativa obligación de proteger dicha información en observancia del</p>

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 12 de 25</p>

CONCEPTO	DESCRIPCIÓN
	marco legal vigente.
Registro Nacional de Bases de Datos	Directorio público de las bases de datos sujetas a Tratamiento que operan en el país (Ley 1581 de 2012, art 25)
Responsable del Tratamiento de Datos	Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3)
Riesgo	Posibilidad de que una entidad 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, proceso, 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)
Titulares de la información	Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
Tratamiento de Datos Personales	Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas (ISO/IEC 27000)

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 13 de 25</p>

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

En esta sección, se documenta de forma estratégica el estado actual de la entidad respecto a la implementación de los lineamientos de seguridad de la información requeridos por el Modelo de Seguridad y Privacidad de la Información -MSPI, actualizado mediante el Anexo1 de la Resolución 500 de 2021 de MINTIC.

Esto permite establecer la línea base donde se encuentra la entidad y así proyectar hacia que punto desea llegar con base a las actividades definidas dentro del Plan de Seguridad y Privacidad de la Información.

El siguiente cuadro revela el nivel de cumplimiento de la entidad en relación con la adopción del modelo:

No.	Evaluación de Efectividad de controles			EVALUACIÓN DE EFECTIVIDAD DE CONTROL
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	57	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	80	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	51	100	EFECTIVO
A.9	CONTROL DE ACCESO	72	100	GESTIONADO
A.10	CRIPTOGRAFÍA	50	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	67	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	61	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	79	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	69	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	60	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	66	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	30	100	REPETIBLE
A.18	CUMPLIMIENTO	76,5	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		64	100	GESTIONADO

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 14 de 25</p>

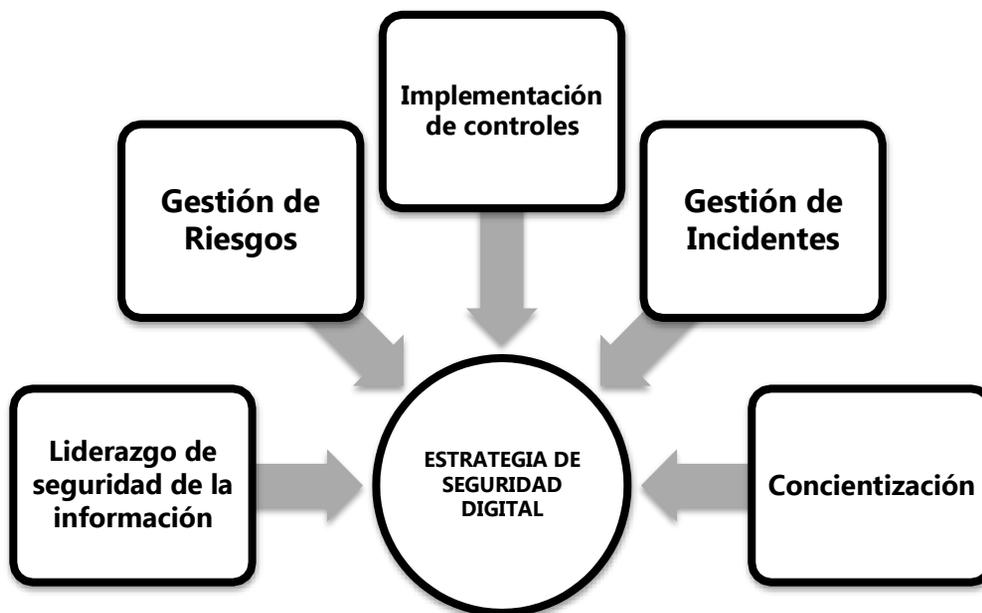
Se puede observar una calificación total de 64 puntos de 100 posibles, lo cual posiciona a la entidad en un nivel “Gestionado”; que muestra que los controles se monitorean y se miden. Por lo anterior se requiere tomar medidas de acción donde los procesos no estén funcionando eficientemente. Por lo anterior, se hace necesario la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, actualizado mediante el Anexo 1 de la Resolución 500 de 2021 de MINTIC y la Resolución N° 746 de 2022, referente a la implementación de controles de protección de la privacidad en aquellos sistemas relacionados con el tratamiento de datos personales.

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 15 de 25</p>

7. ESTRATEGIA DE SEGURIDAD DIGITAL

La estrategia de seguridad digital establecida en la entidad 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 entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, actualizado mediante el Anexo 1 de la Resolución 500 de 2021, así como la Resolución 746 de 2022, la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes.

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



 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 16 de 25</p>

7.1 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 746 de 2022:

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..
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 implementarán 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.

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 17 de 25</p>

8. FASES PARA PLANEAR E INSTRUMENTAR EL MSPI

Las fases necesarias para instrumentar el modelo son:

- Fase de Diagnóstico
- Fase de Planificación
- Fase de Implementación
- Fase de evaluación de desempeño
- Fase de mejora continúa

8.1 FASE DE DIAGNÓSTICO

En esta fase se identifica el estado actual del Instituto Departamental de Salud de Norte de Santander con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información (MSPI), en el cual hace parte integral de la Estrategia de Política de Gobierno Digital.

En la vigencia 2025 se debe aplicar el MSPI de acuerdo a los lineamientos de la Resolución N° 500 de 2021, con el fin de obtener los resultados del nivel de madurez de la entidad.

En la fase de diagnóstico del MSPI el Instituto Departamental de Salud Norte de Santander pretende alcanzar las siguientes metas:

Meta 1: Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad.

Meta 2: Determinar el estado actual de cumplimiento al sistema de protección de datos personales de la entidad, según los lineamientos de la Ley 1581 de 2012.

Meta 3: Identificar el nivel de madurez de seguridad y privacidad de la información en la entidad.

Meta 4: Realizar levantamiento de información para las pruebas de efectividad que permitan a la Entidad medir los controles existentes.

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 18 de 25</p>

8.2 FASE DE PLANIFICACIÓN

Esta fase tiene la finalidad de generar un Plan de Seguridad y Privacidad alineado con el propósito misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

Contexto de la entidad: tiene como fin entender la entidad, sus necesidades, las expectativas y determinar el alcance del MSPI.

Liderazgo: Aquí se muestra el liderazgo y compromiso de la dirección de la entidad, las políticas de seguridad, los roles y responsabilidades de cada uno de los funcionarios.

Planeación: Se planean las acciones con las cuales se abordan los riesgos y oportunidades, objetivos y planes para lograrlos.

Soporte: son los recursos, competencias, sensibilización y documentación.

En la fase de planificación del MSPI el Instituto Departamental de Salud de Norte de Santander pretende alcanzar las siguientes metas:

Meta 1: Elaboración del Plan de comunicaciones

Meta 2: Establecimiento de Roles y Responsabilidades de Seguridad y Privacidad de la Información.

Meta 3: Formulación del plan de cumplimiento al sistema de protección de datos personales de la entidad,

Meta 4: Actualización del inventario de activos de información

Meta 5: Revisión y actualización de la Política de seguridad y privacidad de la información

Meta 6: Seguimiento al Sistema de Gestión de Seguridad Informática

Meta 7: Seguimiento al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 19 de 25</p>

8.3 FASE DE IMPLEMENTACIÓN

En esta fase tomando como base los resultados obtenidos en la fase previa a la planificación del Modelo de Seguridad y Privacidad de la Información (MSPI), y de acuerdo con la identificación de las necesidades de la Entidad, se elabora el plan de Implementación y se ejecuta el plan de tratamiento de riesgos del MSPI.

Plan de implementación

Actualmente, el Instituto Departamental de Salud de Norte de Santander dispone del instrumento Sistema de Gestión de Seguridad Informática (SGSI) y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Versión 04 de enero de 2025. De esta manera se busca la protección de datos dentro de la entidad para garantizar la confidencialidad, integridad y disponibilidad en la toma de decisiones, aportando al mejoramiento continuo y logro de los objetivos estratégicos.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, permite a la entidad controlar que no se presenten cambios que afecten los procesos, tomando acciones para mitigar cualquier evento adverso. En este plan se lleva cada uno de los riesgos a un nivel aceptable.

Se requiere verificar, de acuerdo a una periodicidad establecida, la efectividad de los controles definidos. Para lograr este propósito, la entidad debe construir el Plan de control operacional, el cual permitirá efectuar el monitoreo y seguimiento a los controles de seguridad definidos para los procesos. Los entregables asociados a las metas en la Fase de Implementación deben ser revisados y aprobados por la alta Dirección.

En la fase de implementación se realizan las siguientes metas de acuerdo al resultado de la planeación.

Meta 1: Formulación del Plan de Control Operacional

Meta 2: Implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Meta 3: Seguimiento a Indicadores de Gestión

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 20 de 25</p>

8.4 FASE DE EVALUACIÓN DE DESEMPEÑO

El proceso de seguimiento y monitoreo del MSPI se hace con base en los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la eficacia y efectividad de los controles implementados.

Para definir el plan de seguimiento, evaluación y análisis del MSPI, se requiere dar respuesta a los siguientes interrogantes:

- ¿Qué actividades dentro del MSPI deben ser monitoreadas y evaluadas?
- ¿Qué acciones son necesarias para ese seguimiento y evaluación?
- ¿Quién es el responsable de las acciones de seguimiento y evaluación?
- ¿Cuándo se planifican las acciones de seguimiento y evaluación (oportunidad y periodicidad)?
- ¿Qué metodología se está usando para hacer seguimiento y evaluación del MSPI?
- ¿Qué recursos (financieros, humanos, técnicos, entre otros) se requieren para la ejecución del plan de seguimiento?

La auditoría interna, es un procedimiento que se debe llevar a cabo para la revisión del MSPI implementado, con la finalidad de verificar que los objetivos de control, controles, procesos y procedimientos del MSPI cumplan con los requisitos establecidos en la norma ISO 27002:2013 y los del MSPI.

Para esta fase de evaluación del desempeño se realizan las siguientes metas:

Meta 1: Plan de revisión y seguimiento a la implementación del MSPI

Meta 2: Plan de Ejecución de Auditorias para la revisión del MSPI

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 21 de 25</p>

8.5 FASE DE MEJORA CONTINUA

Esta fase le permitirá al Instituto Departamental de Salud de Norte de Santander, consolidar los resultados obtenidos en la fase de evaluación de desempeño, para diseñar el Plan de Mejoramiento Continuo de Seguridad y Privacidad de la Información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el MSPI.

En esta fase es importante que se defina y ejecute el Plan de Mejora Continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluye:

Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.

Resultados de la auditoria interna al MSPI.

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 22 de 25</p>

9 CRONOGRAMA DE ACTIVIDADES

FASE	ACTIVIDADES	RESPONSABLE	FECHA DE EJECUCIÓN
FASE DE DIAGNÓSTICO	Aplicar la matriz de autodiagnóstico provista por MINTIC, de acuerdo a los lineamientos de la Resolución N° 500 de 2021, para establecer el grado de instrumentación del MSPI y medir el nivel de madurez en seguridad y privacidad.	Todas las dependencias, grupos, subgrupos y Sistemas de Información	Vigencia 2025: Trimestre 1 y 2
	Determinar el estado actual de cumplimiento al sistema de protección de datos personales de la entidad, según los lineamientos de la Ley 1581 de 2012.	Control Interno, Jurídica, Sistemas de Información	Vigencia 2025: Trimestre 1
	Identificación de controles existente para realizar pruebas que permiten medir su efectividad	Planeación, Control Interno, Jurídica, Sistemas de Información	Vigencia 2025: Trimestre 1 y 2
FASE DE PLANIFICACION	Elaboración del Plan de comunicaciones	Planeación y Sistemas de Información	Vigencia 2025: Trimestre 1
	Establecimiento de Roles y Responsabilidades de Seguridad y Privacidad de la Información	Planeación, Control Interno y Sistemas de Información	Vigencia 2025: Trimestre 3
	Actualización de inventario de activos de información	Planeación, Recursos Físicos y Sistemas de Información	Vigencia 2025: Trimestre 1 y 2
	Formulación del plan de cumplimiento al sistema de protección de datos personales de la entidad	Planeación, Jurídica y Sistemas de Información	Vigencia 2025: Trimestre 2

FASE	ACTIVIDADES	RESPONSABLE	FECHA DE EJECUCIÓN
	Revisión y actualización de la Política de seguridad y privacidad de la información	Planeación y Sistemas de Información	Vigencia 2025: Trimestre 4
	Seguimiento al Sistema de Gestión de Seguridad Informática	Comité Institucional de Gestión y Desempeño, Planeación, Control Interno y Sistemas de Información	Vigencia 2025: Trimestre 4
	Seguimiento al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Comité Institucional de Gestión y Desempeño, Planeación, Control Interno y Sistemas de Información	Vigencia 2025: Trimestre 3 y 4
FASE DE IMPLEMENTACIÓN	Formulación del Plan de Control Operacional	Planeación y Sistemas de Información	Vigencia 2025: Trimestre 4
	Implementación del plan de cumplimiento al sistema de protección de datos personales de la entidad	Planeación y Sistemas de Información	Vigencia 2025: Trimestre 3 y 4
	Implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Todas las dependencias, grupos, subgrupos y Sistemas de Información	Vigencia 2026: Trimestre 1 y 2
	Seguimiento a los Indicadores de Gestión	Planeación y Sistemas de Información	Vigencia 2026: Trimestre 1 y 2
FASE DE EVALUACIÓN DE DESEMPEÑO	Elaboración y ejecución de Plan de revisión y seguimiento a la implementación del MSPI	Planeación y Sistemas de Información	Vigencia 2026: Trimestre 3
	Formulación y ejecución de Plan de Ejecución de Auditorías para la revisión del MSPI	Control Interno	Vigencia 2026: Trimestre 2 y 3
FASE DE MEJORA CONTÍNUA	Formulación del plan de mejoramiento continuo de seguridad y privacidad de la información	Planeación y Sistemas de Información	Vigencia 2026: Trimestre 3

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	<p>DIRECCIONAMIENTO ESTRATEGICO</p>	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
<p>Código: F-DE-PE05-04 Versión: 05</p>	<p>COMUNICACION INTERNA</p>	<p>Página 24 de 25</p>

10 RESPONSABLES

- Director Representante Legal de la Entidad: Aprobar los documentos de Alto Nivel.
- Oficina de Planeación: Velar por la implementación del MSPI y garantizar los recursos requeridos.
- Responsable de Seguridad Digital / CIO / Enlace TIC: Coordinar las actividades de implementación del MSPI
- Responsables en Seguridad de la Información formalizados dentro de las políticas de seguridad: Velar por la implementación del MSPI
- Miembros del Comité de gestión y desempeño institucional: Revisión del informe de resultados del análisis de riesgos y gestión de incidentes

 <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p>	DIRECCIONAMIENTO ESTRATEGICO	 <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p>
Código: F-DE-PE05-04 Versión: 05	COMUNICACION INTERNA	Página 25 de 25

11 PLAN DE COMUNICACIÓN

ACTIVIDAD	OBJETIVO	MEDIO	FECHA
Socializar el Plan de Seguridad y Privacidad de la Información	Lograr que todos los funcionarios de la entidad conozcan sus responsabilidades de seguridad de la información	Correos y capacitación	Primero y segundo trimestre de 2025
Crear Talleres para adquirir y ampliar destrezas en seguridad de la información	Crear una cultura preventiva ante posible pérdida de información	Talleres Teórico-Práctico	Tercero y cuarto trimestre de 2025
Realizar boletines informativos por medio de videos	Dar a conocer las amenazas y cómo actuar frente a estas	Correos electrónicos	Primero, segundo y tercer trimestre de 2026
Encuestas de Seguridad de la Información	Conocer la disposición de los funcionarios de la y el nivel de conocimiento adquirido de acuerdo a las actividades realizadas en seguridad de la información	Realiza una encuesta por google medio digital y enviado en link a sus correos y medios de comunicación.	Cuarto trimestre de 2026