# Plan de Privacidad y Seguridad de la Información 2022-2023

***Versión 02***

## GOBIERNO DIGITAL

## INSTITUTO DEPARTAMENTAL DE SALUD DE NORTE DE SANTANDER

**CARLOS ARTURO MARTINEZ GARCIA**
*Director*

**LAURY LISBETH PAEZ PARADA**
*Coordinador Jurídica y Control Disciplinario*

**JOSE TRINIDAD URIBE**
*Coordinador Salud Pública*

**JOSE ANTONIO GUTIERREZ**
*Coordinador Atención en Salud*

**CARMEN ELENA SEPULVEDA AYALA**
*Coordinadora Recursos Financieros*

**HENRY GIOVANNI MANTILLA BLANCO**
*Coordinador Recursos Humanos*

**MARÍA VICTORIA GIRALDO RUIZ**
*Coordinadora de Planeación*

**LUIS ARMANDO ROJAS CAICEDO**
*Líder de Sistemas de Información*

**Enero de 2022**

# Control de Versiones

| Versión | Fecha | Modificación |
|---|---|---|
| **1.0** | Sep - 2020 | PLAN DE SEGURIDAD Y PRIVACIDAD<br>DE LA INFORMACIÓN<br>2020 - 2021 |
| **2.0** | Ene - 2022 | PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN<br>2022 - 2023 |

# Tabla de contenido

# 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.

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

El Modelo está enfocado a preservar la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad. Tomando como elementos esenciales:

- La identificación de riesgos de seguridad digital, que hace un análisis de amenazas y vulnerabilidades en el entorno digital.

- El inventario de Activos de información que involucra los servicios esenciales, humanos y tecnológicos, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

En el presente documento se desarrolla el Plan de Seguridad y Privacidad de la Información del Instituto Departamental de Salud de Norte de Santander, que busca planear y ejecutar todas las fases que permitan la adopción del MSPI.

## 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 2022-2023.

### 2.1 **OBJETIVOS ESPECÍFICOS**

- Definir y establecer la estrategia de seguridad digital de la entidad.
- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos a implementar para la correcta implementación del SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

## 3. ALCANCE

El Plan Estratégico de Seguridad de la Información al buscar la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la entidad, comparte el alcance definido dentro de la Política General de Seguridad de la Información, donde se indica que se tendrán en cuenta todos los procesos de la entidad.

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 2022 y 2023, tiempo necesario para lograr la adopción del MSPI y garantizar su continuidad.

## 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”.
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.

## 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). |

| 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 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. |
| 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) |
| Datos personales | Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012, art 3) |

| 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 intima 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 ambiento propio, particular y privado o semiprivado de una persono natural o |

| CONCEPTO | DESCRIPCIÓN |
|---|---|
| | 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) |
| Información Pública Reservada | 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) |
| Ley de Habeas Data | Se refiere a la Ley Estatutaria 1266 de 2008. |
| Ley de Transparencia y Acceso a la Información Pública | Se refiere a la Ley Estatutaria 1712 de 2014. |
| Mecanismos de protección de datos personales | 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. |
| Plan de continuidad del negocio | 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) |
| Plan de tratamiento de riesgos | 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) |
| Privacidad | 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 |

| 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) |

## 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 Anexo 1 de la Resolución 500 de 2021 de MINTIC.

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

El Instituto Departamental de Salud de Norte de Santander diligenció, en el segundo semestre de 2020, la herramienta denominada INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD, para medir el porcentaje de avance en la planeación y desarrollo del Modelo 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 | | | |
|---|---|---|---|---|
| | DOMINIO | Calificación Actual | Calificación Objetivo | EVALUACIÓN DE EFECTIVIDAD DE CONTROL |
| 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 |


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.

También se emplea como insumo para análisis de la situación actual de la entidad respecto al Sistema de Gestión de Seguridad de la Información, la medición FURAG para la Política

de Seguridad Digital vigencia 2020. De acuerdo a los resultados de esta medición, se hacen las recomendaciones de mejora que se relacionan a continuación:

| RECOMENDACIONES RESULTADOS FURAG VIGENCIA 2020 | |
|---|---|
| **#** | **Recomendaciones** |
| **1** | Incluir la forma en que se le dará tratamiento a los riesgos (evitar, compartir, reducir y aceptar) dentro de la política de administración de riesgos establecida por la alta dirección y el comité institucional de coordinación de control interno. |
| **2** | Establecer el nivel de aceptación del riesgo dentro de la política de administración de riesgos establecida por la alta dirección y el comité institucional de coordinación de control interno. |
| **3** | Establecer niveles para calificar el impacto del riesgo dentro de la política de administración de riesgos establecida por la alta dirección y el comité institucional de coordinación de control interno. |
| **4** | Fomentar la promoción de los espacios para capacitar a los líderes de los procesos y sus equipos de trabajo sobre la metodología de gestión del riesgo con el fin de que sea implementada adecuadamente entre los líderes de proceso y sus equipos de trabajo, por parte del comité institucional de coordinación de control interno. |
| **5** | Describir como se realiza la actividad de control, por parte de los líderes de los programas, proyectos, o procesos de la entidad y en coordinación con sus equipos de trabajo, al momento de diseñar los controles. |

| | |
|---|---|
| **6** | Proporcionar una descripción del manejo frente a observaciones o desviaciones resultantes de la ejecución del control con el fin de dar lineamientos sobre los posibles cursos de acción, por parte de los líderes de los programas, proyectos, o procesos de la entidad y en coordinación con sus equipos de trabajo, al momento de diseñar los controles. |
| **#** | **Recomendaciones** |
| **7** | Hacer seguimiento a los riesgos y controles de sus procesos, programas o proyectos a cargo, por parte de los líderes de los programas, proyectos, o procesos de la entidad en coordinación con sus equipos de trabajo. |
| **8** | Contemplar evaluaciones para monitorear el estado de los componentes del sistema de control interno, dentro de la evaluación a la gestión del riesgo que hacen los jefes de planeación, líderes de otros sistemas de gestión o comités de riesgos. |
| **9** | Contemplar la elaboración de informes a las instancias correspondientes sobre las deficiencias de los controles, dentro de la evaluación a la gestión del riesgo que hacen los jefes de planeación, líderes de otros sistemas de gestión o comités de riesgos. |
| **10** | Identificar factores sociales que pueden afectar negativamente el cumplimiento de los objetivos institucionales. Desde el sistema de control interno efectuar su verificación. |
| **11** | Evaluar por parte del jefe de control interno o quien haga sus veces en la entidad, que los controles diseñados indiquen qué pasa con las observaciones o desviaciones resultantes de ejecutar el control. |

| | |
|---|---|
| **12** | Evaluar por parte del jefe de control interno o quien haga sus veces en la entidad, que los controles diseñados soporten evidencia de la ejecución del control. |
| **13** | Elaborar el plan operacional de seguridad y privacidad de la información de la entidad, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua. |
| **#** | **Recomendaciones** |
| **14** | Fortalecer las capacidades en seguridad digital de la entidad a través de su participación en las jornadas de sensibilización y capacitaciones del uso seguro de entorno digital convocadas por el Ministerio de Tecnologías de la Información y las Comunicaciones. |
| **15** | Fortalecer las capacidades en seguridad digital de la entidad a través de convenios o acuerdos de intercambio de información para fomentar la investigación, la innovación y el desarrollo de temas relacionados con la defensa y seguridad nacional en el entorno digital. |
| **16** | Fortalecer las capacidades en seguridad digital de la entidad a través de ejercicios de simulación de incidentes de seguridad digital al interior de la entidad. |
| **17** | Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como registrarse en el CSIRT Gobierno y/o ColCERT. |

| | |
|---|---|
| **18** | Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como adoptar e implementar la guía para la identificación de infraestructura crítica cibernética. |
| **19** | Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como realizar la identificación anual de la infraestructura crítica cibernética e informar al CCOC. |
| **20** | Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en la contrucción de los planes sectoriales de protección de la infraestructura crítica cibernética. |
| **#** | **Recomendaciones** |
| **21** | Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como adoptar e implementar la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en entidades públicas. |
| **22** | Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en las mesas de construcción y sensibilización del Modelo Nacional de Gestión de Riesgos de Seguridad Digital. |
| **23** | Hacer campañas de concientización en temas de seguridad de la información de manera frecuente y periódica, específicas para cada uno de los distintos roles dentro de la entidad. |

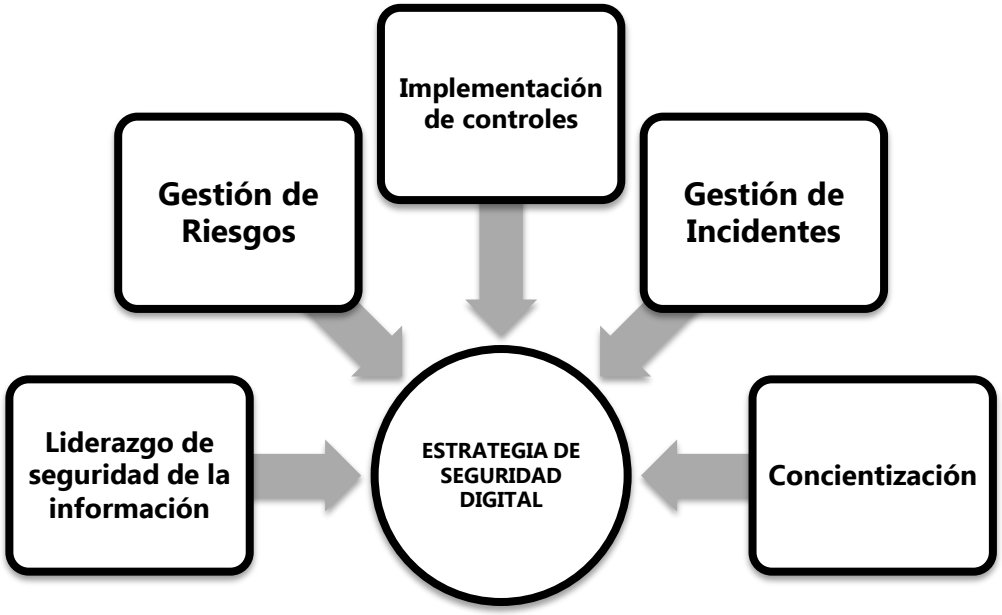
| | |
|---|---|
| **24** | Establecer un procedimiento de gestión de incidentes de seguridad de la información, formalizarlo y actualizarlo de acuerdo con los cambios de la entidad. |
| **25** | Efectuar evaluaciones de vulnerabilidades informáticas. |
| **26** | Cerciorarse de que los proveedores y contratistas de la entidad cumplan con las políticas de ciberseguridad internas. |
| **27** | Realizar retest para verificar la mitigación de vulnerabilidades y la aplicación de actualizaciones y parches de seguridad en sus sistemas de información. |
| **#** | **Recomendaciones** |
| **28** | Realizar periódicamente ejercicios simulados de ingeniería social al personal de la entidad incluyendo campañas de phishing, smishing, entre otros, y realizar concientización, educación y formación a partir de los resultados obtenidos. |
| **29** | Realizar copias de respaldo con una periodicidad definida con los usuarios de la información y realizar pruebas de restauración de las copias para garantizar su correcto funcionamiento en caso de que sean requeridas. |

Con base en los resultados obtenidos en la aplicación del instrumento de evaluación Modelo de Seguridad y Privacidad de la Información y los resultados de la medición FURAG vigencia 2020 para los temas de seguridad de la información, se requiere tomar medidas de acción donde los procesos no estén funcionando eficientemente. Por lo cual, 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.

## 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 de 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:



## 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 y la resolución 500 de 2021:

| 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 tendiendo 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. |

## 8. FASES PARA PLANEAR E INSTRUMENTAR EL MSPI

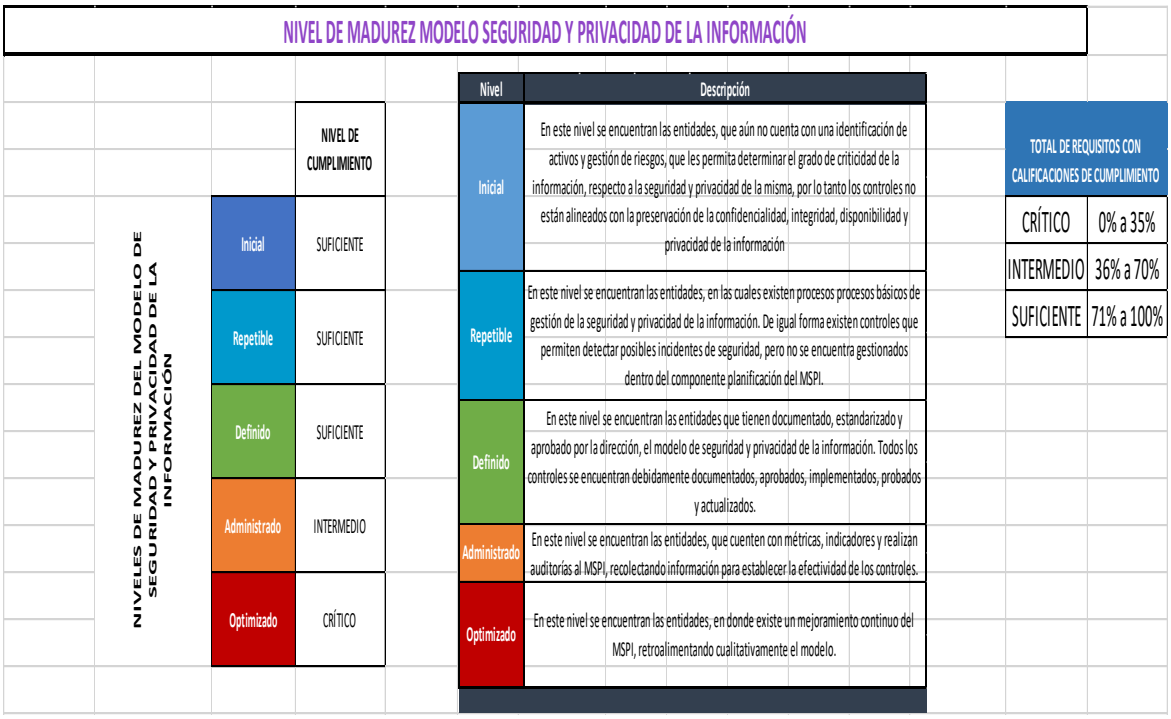
Las fases necesarias para instrumentar el modelo son:

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

### 8.1 FASE 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.

El Instituto Departamental de Salud Norte de Santander aplicó en la vigencia 2020 el MSPI, con el fin de identificar el nivel de madurez en seguridad y privacidad de la información. La siguiente gráfica nos ilustra:




En la vigencia 2022 se debe aplicar nuevamente el MSPI de acuerdo a los lineamientos de la Resolución n° 500 de 2021, con el fin de actualizar los resultados del nivel de madurez.

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

Meta 3: Realizar levantamiento de información para las pruebas de efectividad que permitan a la Entidad medir los controles existentes.

## 8.2 FASE 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: en este lo que se pretende es 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: Actualización de inventario de activos de información

Meta 4: Revisión y actualización de la Política de seguridad y privacidad de la información

Meta 5: Seguimiento al Sistema de Gestión de Seguridad Informática

Meta 6: Seguimiento al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Meta 7: Desarrollar las actividades de la fase 1 Planeación de IPv6, de acuerdo a las recomendaciones de la Guía de Transición de IPv4 a IPv6 para Colombia, actualizadas mediante Resolución N° 01126 DE 2021 - Mintic

## 8.3 FASE 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 03 de Enero de 2022. 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, según el anexo A de la Norma ISO 27000:2017 y la guía de controles sobre privacidad del MSPI.

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

Meta 4**:** Desarrollar las actividades de la fase 2 Implementación de IPv6, en convivencia con el protocolo IPv4, de acuerdo a las recomendaciones de la Guía de Transición de IPv4 a IPv6 para Colombia, actualizadas mediante Resolución N° 01126 DE 2021 - Mintic

## 8.4 FASE EVALUACIÓN DE DESEMPEÑO

El proceso de seguimiento y monitoreo del MSPI se hace con base en los resultados que arroja 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

## 8.5 FASE 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.

## 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 2022: Trimestre 1 y 2 |
| | Identificación de controles existentes para realizar pruebas que permite medir su efectividad | Planeación, Control Interno, Jurídica, Sistemas de Información | Vigencia 2022: Trimestre 1 y 2 |
| FASE DE PLANIFICACION | Elaboración del Plan de comunicaciones | Planeación y Sistemas de Información | Vigencia 2022: Trimestre 1 |
| | Establecimiento de Roles y Responsabilidades de Seguridad y Privacidad de la Información | Planeación, Control Interno, Sistemas de Información | Vigencia 2022: Trimestre 3 |
| | Actualización de inventario de activos de información | Planeación, Recursos Físicos, Sistemas de Información | Vigencia 2022: Trimestre 1 y 2 |

| FASE | ACTIVIDADES | RESPONSABLE | FECHA DE EJECUCIÓN |
|---|---|---|---|
| | Revisión y actualización de la Política de seguridad y privacidad de la información | Planeación, Sistemas de Información | Vigencia 2022: Trimestre 4 |
| | Seguimiento al Sistema de Gestión de Seguridad Informática | Comité Institucional de Gestión y Desempeño, Planeación, Control Interno, Sistemas de Información | Vigencia 2022: 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, Sistemas de Información | Vigencia 2022: Trimestre 3 y 4 |
| | Desarrollar las actividades de la fase 1 Planeación de IPv6, de acuerdo a las recomendaciones de la Guía de Transición de IPv4 a IPv6 para Colombia, actualizadas mediante Resolución N° 01126 DE 2021 - Mintic | Planeación y Sistemas de Información | Vigencia 2022: Trimestre 1 y 2 |
| FASE DE IMPLEMENTACION | Formulación del Plan de Control Operacional | Planeación y Sistemas de Información | Vigencia 2022: Trimestre 4 |
| | Implementación del plan de tratamiento de riesgos de | Todas las dependencias, | Vigencia 2023: |

| FASE | ACTIVIDADES | RESPONSABLE | FECHA DE EJECUCIÓN |
|---|---|---|---|
| | Seguridad y Privacidad de la Información | grupos, subgrupos y Sistemas de Información | Trimestre 1 y 2 |
| | Seguimiento a los Indicadores De Gestión | Planeación, Sistemas de Información | Vigencia 2023: Trimestre 1 y 2 |
| | Desarrollar las actividades de la fase 2 Implementación de IPv6, en convivencia con el protocolo IPv4, de acuerdo a las recomendaciones de la Guía de Transición de IPv4 a IPv6 para Colombia, actualizadas mediante Resolución N° 01126 DE 2021 - Mintic | Planeación, Sistemas de Información | Vigencia 2022: Trimestre 3 y 4<br><br>Vigencia 2023: Trimestre 1 y 2 |
| FASE EVALUACIÓN DE DESEMPEÑO | Elaboración y ejecución de Plan de revisión y seguimiento a la implementación del MSPI | Planeación y Sistemas de Información | Vigencia 2023: Trimestre 3 |
| | Formulación y ejecución de Plan de Ejecución de Auditorias para la revisión del MSPI | Control Interno | Vigencia 2023: Trimestre 2 y 3 |
| FASE DE MEJORA CONTINUA | Formulación del plan de mejoramiento continuo de seguridad y privacidad de la información | Planeación y Sistemas de Información | Vigencia 2023: Trimestre 3 |

## 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
- 

## 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 2022 |
| Crear Talleres para adquirir y ampliar destrezas en seguridad de la información | Crear una cultura preventiva ante posibles perdida de información | Talleres Teórico-Práctico | Tercero y cuarto trimestre de 2022 |
| 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 2023 |
| 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 2023 |