PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2020 - 2021

San José de Cúcuta, Septiembre de 2020

MIEMBROS DEL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

Director. - Presidente	Dr. Carlos Arturo Martínez García
Coordinador de Planeación. – Secretaria Técnica	María Victoria Giraldo Ruiz
Funcionario responsable de sistemas de información	Maricela Villegas Guisao
Coordinadora recursos Financieros	Carmen Elena Sepúlveda
Coordinador recursos Humanos	Henry Giovanni Mantilla Blanco
Coordinador Grupo Atención en salud	José Antonio Gutiérrez
Coordinador Grupo Salud pública	José Trinidad Uribe Navarro
Coordinador de la oficina de Control Jurídica y Control Interno Disciplinario	Laury Lisbeth Páez Parada Ana Edilia Carrero

INVITADOS ESPECIALES COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

Recursos Físicos, Participación Social, Oficina SAC, Grupo atención en salud	Omaira Torrado
Sub grupo Vigilancia y control	Gloria Montaño
Responsable subgrupo Prestación de Servicios	Sigward Peñaloza Echavez

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), propone El Modelo de Seguridad y Privacidad de la Información - MSPI, el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI.

El MSPI está acorde con las buenas prácticas de seguridad reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

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. JUSTIFICACIÓN

En la actualidad son muchas las amenazas y vulnerabilidades que pueden afectar los activos de información, por eso se debe proteger y garantizar la calidad, autenticidad y privacidad de estos, para El Instituto Departamental de Salud de Norte de Santander es vital adelantar todas las medidas necesarias que logren este propósito.

La política de Gobierno Digital es un eje que permite impulsar el desarrollo de la gestión de la entidad. Dentro de las acciones orientadas a planear la política de Gobierno Digital en cada entidad se encuentra la revisión del estado de implementación del Modelo de Seguridad y Privacidad de la Información –MSPI.

Esta implementación, está determinada por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la entidad, con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

En el plan de seguridad se establecen los detalles de cómo se realizará la implementación de la seguridad de la información en cada uno de los procesos de la entidad, estipulando directrices, tiempo, responsables y productos concretos a entregar en la vigencia para lograr un adecuado proceso de gestión, administración y evaluación de la entidad.

3. ALCANCE

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 2020 y 2021, tiempo necesario para lograr la adopción del MSPI y garantizar su continuidad.

4. 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).
Auditoría	Proceso sistemático, independiente y documentado para obtener evidencias de

CONCEPTO	DESCRIPCIÓN
	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)
Datos personales Públicos	Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre

CONCEPTO	DESCRIPCIÓN
	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 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

CONCEPTO	DESCRIPCIÓN
	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 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

CONCEPTO	DESCRIPCIÓN
	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)

5. MARCO LEGAL Y DOCUMENTOS DE REFERENCIA

La normatividad aplicable al Plan de seguridad y privacidad de la información es:

NORMA	DESCRIPCION
Ley 1581 de 2012	Por la cual se dictan disposiciones para la protección de datos personales
Decreto 1377 de 2013	Por medio del cual se reglamenta parcialmente la ley 1581 de 2012
Ley 1712 de 2014	Ley de transparencia y derecho de acceso a la información pública
Conpes 3854 de 2016	Por medio del cual se establece la política nacional de seguridad digital
Decreto 1413 de 2017	Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Decreto 612 de abril 4 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
Decreto 1008 de Junio de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Decreto 2106 de 2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
Manual de Gobierno Digital	Implementación de la política de Seguridad de la Información
Guía para la administración del riesgo	Anexo 4 Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas
PETI 2020 - IDS	Plan Estratégico de Tecnologías de la Información Instituto Departamental de Salud, Norte de Santander 2020
SGSI 2020 - IDS	Sistema de Gestión de Seguridad Informática y Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información - IDS, Versión 02

6. OBJETIVOS

6.1 OBJETIVO GENERAL

Planificar, orientar y construir el plan general de seguridad y privacidad del Instituto Departamental de Salud de Norte de Santander, de acuerdo a los lineamientos de Mintic y las normas legales, con el fin de proteger la integridad y garantizar la disponibilidad y confidencialidad de la información.

6.2 OBJETIVOS ESPECÍFICOS

- Crear los procedimientos, instrumentos, acciones y responsabilidades del personal del Instituto Departamental de Salud Norte de Santander, frente a la garantía de la seguridad de la información.

- Enunciar el proyecto de seguridad de la información de acuerdo a las necesidades y prioridades del Instituto Departamental de Salud Norte de Santander.

- Programar la ejecución del plan de seguridad con sus respectivas actividades y documentación correspondiente.

7. ANÁLISIS DE LA SITUACIÓN ACTUAL

El Instituto Departamental de Salud de Norte de Santander diligenció 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

Como la calificación total arrojo un valor de 64 puntos de 100 posibles, posiciona a la entidad en un nivel "Gestionado"; que muestra que en la entidad los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente. Por lo tanto se hace necesario planear y desarrollar el modelo a través de la aplicación de las diferentes guías que ha entregado el Ministerio de las Tecnologías de la Información y las Comunicaciones para este fin. Se busca habilitar la Política de Gobierno Digital a través de la plena identificación y protección de los activos de información de la entidad.

8. FASES PARA PLANEAR E INSTRUMENTAR EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 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 pretende identificar 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, que de ahora en adelante se denominará MSPI, en el cual hace parte integral de la Estrategia de Política de Gobierno Digital.

Estado actual de la entidad: El Instituto Departamental de Salud Norte de Santander actualmente ha trabajado sobre los diferentes planes emitidos por la Política de Gobierno Digital, porque es necesario que la entidad este a la vanguardia en pro de la seguridad de la información.

Identificar el nivel de madurez: La siguiente gráfica nos ilustra

NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	SUFICIENTE
Definido	SUFICIENTE
Administrado	INTERMEDIO
Optimizado	CRÍTICO

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

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: Autodiagnóstico Transición de IPv4 a IPv6

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 02 de Enero de 2020. 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 27001:2013 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**:** Plan de Transición de IPv4 a IPv6

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 INICIO
FASE DE DIAGNÓSTICO	Aplicar la matriz de autodiagnóstico provista por MINTIC 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	Ya realizado
	Identificación de controles existentes para realizar pruebas que permite medir su efectividad	Planeación, Control Interno, Jurídica, Sistemas de Información	Septiembre de 2020
FASE DE PLANIFICACION	Elaboración del Plan de comunicaciones	Planeación y Sistemas de Información	Ya realizado
	Establecimiento de Roles y Responsabilidades de Seguridad y Privacidad de la Información	Planeación, Control Interno, Sistemas de Información	Septiembre de 2020
	Actualización de inventario de activos de información	Planeación, Recursos Físicos, Sistemas de Información	Octubre de 2020
	Revisión y actualización de la Política de seguridad y privacidad de la información	Planeación, Sistemas de Información	Noviembre de 2020
	Seguimiento al Sistema de Gestión de Seguridad Informática	Comité Institucional de Gestión y Desempeño, Planeación, Control Interno,	Diciembre de 2020

FASE	ACTIVIDADES	RESPONSABLE	FECHA DE INICIO
		Sistemas de Información	
	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	Diciembre de 2020
	Autodiagnóstico Transición de IPv4 a IPv6	Todas las dependencias, grupos, subgrupos y Sistemas de Información	Enero de 2021
FASE DE IMPLEMENTACION	Formulación del Plan de Control Operacional	Planeación y Sistemas de Información	Febrero de 2021
	Implementación del plan de tratamiento de riesgos de Seguridad y Privacidad de la Información	Todas las dependencias, grupos, subgrupos y Sistemas de Información	Marzo de 2021
	Seguimiento a los Indicadores De Gestión	Planeación, Sistemas de Información	Abril de 2021
	Elaboración del Plan de Transición de IPv4 a IPv6	Planeación, Sistemas de Información	Mayo de 2021
FASE EVALUACIÓN DE DESEMPEÑO	Elaboración y ejecución de Plan de revisión y seguimiento a la implementación del MSPI	Planeación y Sistemas de Información	Mayo de 2021

FASE	ACTIVIDADES	RESPONSABLE	FECHA DE INICIO
	Formulación y ejecución de Plan de Ejecución de Auditorias para la revisión del MSPI	Control Interno	Mayo de 2021
FASE DE MEJORA CONTINUA	Formulación del plan de mejoramiento continuo de seguridad y privacidad de la información	Planeación y Sistemas de Información	Junio de 2021

10. 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	Octubre de 2020
Crear Talleres para adquirir y ampliar destrezas en seguridad de la información	Crear una cultura preventiva ante posibles perdida de información	Talleres Teórico-Práctico	Primer semestre de 2021
Realizar boletines informativos por medio de videos	Dar a conocer las amenazas y cómo actuar frente a estas	Correos electrónicos	Primer semestre de 2021
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.	Primer semestre de 2021

MARICELA VILLEGAS GUISAO
P.U. Sistemas de Información

Elaboró y Proyectó: V. Núñez
Revisó: M. Villegas