HOSPITAL UNIVERSITARIO
DEPARTAMENTAL DE NARIÑO E.S.E.

ACREDITACION EN SALUD

¡Trabajamos por mi Nariño,
tu salud,
nuestro compromiso!

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E.

2024

TABLA DE CONTENIDO

1	INTRODUCCION	5
2,1	OBJETIVO	6
2,2	OBJETIVOS ESPECIFICOS	6
3	ALCANCE	6
4	JUSTIFICACIÓN	7
5	DEFINICIONES	7
6	ROL DE LA ALTA DIRECCION	14
7	MODELO PHVA VERSUS SGSI	14
8	GUIAS DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	15
8.1.	MODELO	18
8.2.	FASE I Diagnóstico	21
8.3.	FASE II Planificación	22
8.4.	FASE III Implementación	24
8.5.	FASE IV Evaluación De Desempeño	25
8.5.	FASE V Mejora Continua	25
	CONTROL DE CAMBIOS	28

INDICE DE TABLAS

Tabla 1: Guías del MSPI_____ 15
Tabla 2: Corresponsabilidad ISO IEC:27001_____ 20
Tabla 3: Metas del Diagnóstico_____ 21
Tabla 4: Metas de la Planificación_____ 22
Tabla 5:Metas de la Implementación_____ 24
Tabla 6: Metas de la Evaluación de Desempeño_____ 25
Tabla 7: Meta del Mejoramiento Continuo_____ 26
Tabla 8: Cronograma de Desarrollo de Actividades_____ 27

INDICE DE FIGURAS

Figura 1: Modelo PHVA Aplicado a SGSI_____ 14
Figura 2: Ciclo de Operación del MSPI_____ 18
Figura 3: Fases Del MSPI Versus ISO-IEC 27001_____ 20

1. INTRODUCCION

Este documento se elaboró teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información, en adelante MSPI, desarrollado para apoyar uno de los ejes transversales de la Política Gobierno Digital, este modelo se basa en cinco fases las cuales son diagnóstico, planificación, implementación, gestión y mejoramiento continuo, las cuales a su vez se alinean con la NTC/IEC ISO 27001.

La estrategia de Gobierno Digital, la cual es liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado y Sociedad más participativos, más eficientes y más transparentes.

El MSPI contribuye a que se garantice la confidencialidad, integridad y disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo asociado al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, lo que permite establecer entornos de confianza digital entre las partes interesadas y que hacen uso de la tecnología para el intercambio de información.

El Modelo de Seguridad y Privacidad de la Información consta de varios documentos asociados (Guías) las cuales se deben utilizar para mejorar los estándares de Seguridad y Privacidad de la información y se convierten en el instrumento adecuado para formular el presente documento del Plan de Seguridad y Privacidad de la Información.

Como metodología es importante tener presente que las guías se desarrollan en cada una de las fases del modelo y dan los lineamientos para saber cuáles son los resultados a obtener y como desarrollarlos.

2. OBJETIVO

2.1. OBJETIVO GENERAL

El Plan de Seguridad y Privacidad de la información se crea para fortalecer el sistema de información interno, para dar cumplimiento a las políticas de gobierno corporativo, se asume retos de implementar métodos para garantizar la seguridad, confidencialidad, integridad y disponibilidad de la información.

2.2. OBJETIVOS ESPECIFICOS

- Mantener el Plan de Seguridad y Privacidad de la Información, el cual debe estar alineado con el plan de acción del HUDN y orientado a garantizar la confidencialidad, integridad y disponibilidad de los activos de información conforme a la matriz de riesgos de GI.
- Proponer y promover mejores prácticas de seguridad informática en la institución.
- Guiar al personal del hospital en el comportamiento profesional del manejo de la información interna, y así evitar la pérdida de información.
- Mantener al interior del hospital actualizado todo lo concerniente a normalización en el tratamiento y privacidad de la información.

3. ALCANCE

El presente plan cubre las vigencias de los periodos 2023 y 2024, en este documento se refleja los principales lineamientos para garantizar la Seguridad y Privacidad de La Información y aplica a todos los procesos de la organización definidos en el mapa de procesos, siendo estos de dirección, de evaluación, misionales y de apoyo, por otra parte las directrices y actividades que resulten del presente plan deben ser divulgados, conocidos y cumplidos por todos los colaboradores de la entidad, contratistas y en general todos los terceros que tengan acceso, almacenen, procesen o trasmitan información de la entidad y/o de los usuarios.

4. JUSTIFICACIÓN

El presente plan de seguridad de la información se define en cumplimiento a su propósito y obligación interna como sectorial, en la contribución a la construcción de un estado más eficiente, transparente y participativo a través de la definición del plan de seguridad y privacidad de la información, al igual que a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de Gobierno Digital.

5. DEFINICIONES

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, etc.) que tenga valor para la organización. (NTC/IEC ISO 27001).

Activo de Información: Un activo de información en el contexto de la norma ISO/IEC 27001 es: "algo que una organización valora y por lo tanto debe proteger", es un dato creado o utilizado para el procesamiento, trasporte o almacenamiento de información.

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: Situaciones que desencadenan en un incidente en la empresa, realizando un daño material o pérdidas inmateriales de sus activos de información. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Vulnerabilidad: es la potencialidad o la posibilidad de que se materialice una amenaza sobre dicho activo (ISO/IEC 27000).

Matriz de riesgos: herramienta de análisis de riesgos que sirve para evaluar la probabilidad y la gravedad del riesgo durante el proceso de planificación del proyecto.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (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 (Ley 1581 de 2012, art 3).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto 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 datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la 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 otros, los datos relativos al estado civil de las personas, a su profesión u 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: Para efectos de esta guía 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, la 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).

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por 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 un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona 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 de 2014, 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 constituyen 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.

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Plan de continuidad del negocio: Plan orientado a permitir la 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 la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL 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).

Responsabilidad Demostrada: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

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 amenaza 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, procesos, 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).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

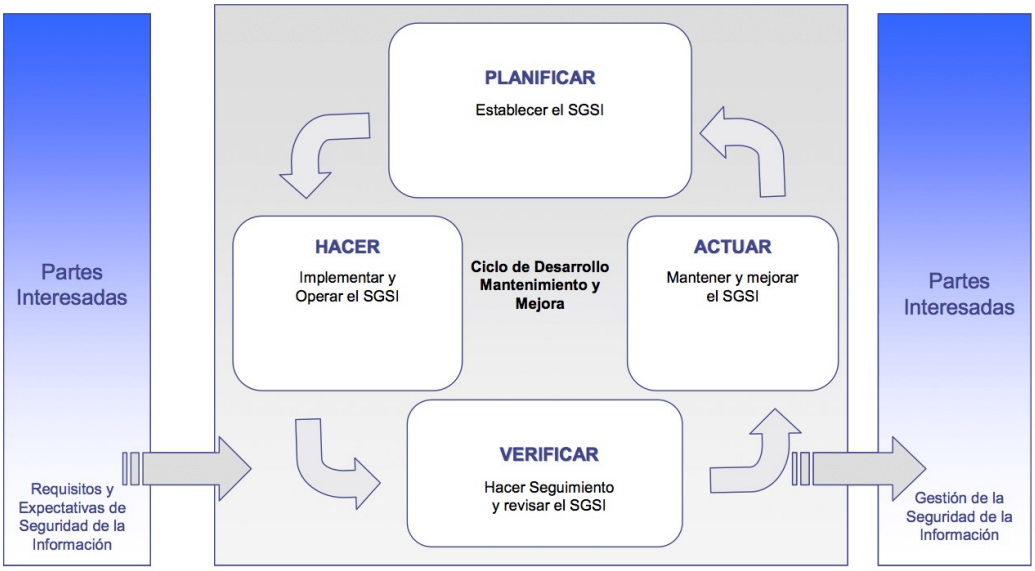
6. ROL DE LA ALTA DIRECCION

La Alta Dirección del Hospital Universitario Departamental de Nariño E.S.E. manifiesta el compromiso y apoyo en el diseño, implementación y mantenimiento del Sistema de Gestión de Seguridad y Privacidad de la Información, definiendo la política de seguridad de la información, estableciendo los lineamientos de seguridad, fijando el gobierno de seguridad y la asignación de los recursos necesarios para llevar a feliz término las actividades programadas.

7. MODELO PHVA VERSUS SGSI

Para poder desarrollar el MSPI este documento se basa en el modelo PHVA que se ilustra en el siguiente gráfico.

Figura 1: Modelo PHVA Aplicado a SGSI



8. GUIAS DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Como el MSPI es basado en ISO-IEC 27001, el Ministerio de Tecnologías de la Información y las Comunicaciones MinTic, ha desarrollado una serie de guías que deben ser desarrolladas para lograr que el MSPI dentro de la organización quede establecido e implementado.

Tabla 1: Guías del MSPI

GUIA	TITULO GUIA	OBJETIVO DE LA GUÍA
Guía 1	Metodología de pruebas de efectividad	Indicar los procedimientos de seguridad que pueden generarse durante el proceso de evaluación en los avances en la implementación del modelo de seguridad y privacidad de la información
Guía 2	Política General MSPI	Establecer lineamientos para la elaboración de la política general de seguridad y privacidad de información para las entidades públicas, como parte del Modelo de Seguridad y Privacidad de la Información de la política Gobierno Digital
Guía 3	Procedimientos de Seguridad y Privacidad de la Información	Indicar los procedimientos de seguridad que pueden generarse durante el diseño y la implementación del modelo de seguridad y privacidad de la información para las entidades del estado
Guía 4	Roles y responsabilidades de seguridad y privacidad de la información	Definir el equipo responsable de seguridad y privacidad de información dentro de las entidades públicas, como parte del Modelo de Seguridad y Privacidad de la Información
Guía 5	Gestión de Activos	Brindar los lineamientos básicos que deben ser utilizados por los responsables de la seguridad de la información, para poner en marcha la gestión y clasificación de activos de información que son manejados por la organización

Guía 6	Gestión Documental	Presentar una relación de la Normatividad Técnica Colombiana – NTC, de acuerdo con los lineamientos establecidos por el Archivo General de la Nación
Guía 7	Gestión de Riesgos	Orientar a las Entidades a gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP
Guía 8	Controles de Seguridad	Proteger la información de las entidades del Estado, los mecanismos utilizados para el procesamiento de la información, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información
Guía 9	Indicadores Gestión SI	Evaluar la efectividad de la implementación de los controles de seguridad y evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la entidad
Guía 10	Continuidad de TI	Establecer procedimientos específicos que respondan a interrupciones del servicio, con el fin de proteger y recuperar las funciones críticas del negocio que se puedan ver comprometidas por eventos naturales, o sean ocasionados por el hombre
Guía 11	Impacto Negocio	Disponer de un documento guía por medio del cual las Entidades del estado puedan consultar los lineamientos de seguridad ante situaciones de emergencia a fin de mitigar el impacto producido por la interrupción de los servicios de alta criticidad que afectan sensiblemente las operaciones del negocio
Guía 12	Seguridad en la Nube	Este documento, presenta los lineamientos y aspectos a tener en cuenta para el aseguramiento de la información en la nube – Cloud; que las Entidades del Estado deben seguir, de tal manera que se conserve la seguridad de los datos en este tipo de ambientes
Guía 13	Guía De Evidencia Digital	Indicar a las diferentes entidades del estado, como llevar a cabo una correcta identificación, recolección, análisis y manipulación de datos en caso de algún evento o incidente de seguridad que requiera de evidencias digitales para su investigación

Guía 14	Plan de comunicación, sensibilización y capacitación	Este documento tiene como objetivo establecer lineamientos para la construcción y mantenimiento del plan de capacitación, sensibilización y comunicación de la seguridad de la información, para así asegurar que este, cubra en su totalidad los funcionarios de la Entidad, asegurando que cada uno cumpla con sus roles y responsabilidades
Guía 15	Auditoria	Indicar los procedimientos de Auditoria en el proceso de verificación de la implementación del modelo de seguridad y privacidad de la información
Guía 16	Evaluación del Desempeño	El propósito ofrecer recomendaciones para la correcta evaluación del desempeño de la Seguridad y Privacidad de la Información de la Entidad que previamente ha planeado, implementado y gestionado el MSPI
Guía 17	Mejora Continua	Ofrecer una serie de recomendaciones para el mantenimiento y mejora de la Seguridad y Privacidad de la Información de Entidad que previamente ha planeado, implementado y gestionado el MSPI
Guía 18	Lineamientos terminales de áreas financieras entidades públicas	Dar lineamientos que las entidades deben implementar para elevar el aseguramiento de los equipos o terminales móviles asignados por la entidad, donde se realizan las transacciones a financieras como los son: pago de nómina, pagos de seguridad social, pagos de contratación y transferencias de fondos, entre otros
Guía 19	Aseguramiento del protocolo IPV6	Presentar un marco de referencia sobre lineamientos de seguridad en IPv6, que sea referente para abordar el plan de diagnóstico, plan de implementación y monitoreo del proceso de transición de IPv4 a IPv6 en cada una de las Entidades
Guía 20	Transición IPv4_IPv6	Presentar un marco de referencia para facilitar el proceso de transición de IPv4 a IPv6, que permita orientar a las Entidades del Gobierno y a la sociedad en general, en el análisis, la planeación, la implementación y las pruebas de funcionalidad del protocolo IPv6, con el fin de incentivar el proceso de adopción y despliegue del protocolo IPv6 en el país
Guía 21	Gestión de Incidentes	El objetivo principal del Modelo de Gestión de Incidentes de seguridad de la información es tener un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información

9. MODELO

El Modelo de Seguridad y Privacidad de la Información define un ciclo de operación que consta de cinco (5) fases, como se muestra en la siguiente figura; las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información y esta como el componente principal de la política Gobierno Digital enfocado a preservar la confidencialidad, integridad y disponibilidad de la información.

Figura 2: Ciclo de Operación del MSPI

Fuente: Guía del MSPI del MinTic

Fase I Diagnostico: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Fase II Planificación (Planear): Que hace referencia a establecer el Modelo de Seguridad y Privacidad de la Información, en esta fase se debe establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar los activos y el riesgo buscando mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de la entidad.

Fase III Implementación (Hacer): Que hace referencia a implementar u operar el MSPI, en esta fase se debe implementar y operar la política, los controles y procedimientos del MSPI.

Fase IV Evaluación de Desempeño (Verificar): Que hace referencia a hacer seguimiento y revisión del MSPI, en esta fase se debe evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.

Fase V Mejora Continua (Actuar): Que hace referencia a mantener y mejorar el MSPI, en esta fase de debe emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del MSPI y la revisión por la dirección, para lograr la mejora continua del MSPI.

Figura 3: Fases Del MSPI Versus ISO-IEC 27001

Fuente: Guía del MSPI del MinTic

Tabla 2: Corresponsabilidad ISO IEC: 27001

FASES CICLO DE OPERACIÓN MSPI	CORRESPONSABILIDAD CON ISO 27001:2013
DIAGNOSTICO	En la norma ISO 27001:2013. En el capítulo 4 - Contexto de la organización de la norma ISO 27001:2013, se determina la necesidad de realizar un análisis de las cuestionas externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesas de la organización en el alcance del SGSI.
PLANIFICACION	En la norma ISO 27001:2013. En el capítulo 5 - Liderazgo, se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la organización asegure la asignación de los recursos para el SGSI y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen.
	En el capítulo 6 - Planeación, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.

	En el capítulo 7 - Soporte se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua Sistema de Gestión de Seguridad de la Información.
IMPLEMENTACION	En la norma ISO 27001:2013. En el capítulo 8 - Operación de la norma ISO 27001:2013, se indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.
EVALUACION DEL DESEMPEÑO	En la norma ISO 27001:2013. En el capítulo 9 - Evaluación del desempeño, se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.
MEJORA CONTINUA	En la norma ISO 27001:2013. En el capítulo 10 - Mejora, se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información, que a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectiva para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

8.1. FASE I Diagnóstico

Objetivo: En esta fase lo que se pretende es establecer el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Tabla 3: Metas del Diagnóstico

METAS	INSTRUMENTOS O HERRAMIENTAS A UTILIZAR	RESULTADOS ESPERADOS
Determinar el estado actual de la gestión de seguridad y privacidad de la información al	Diagnostico nivel de cumplimiento de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la norma ISO 27001:2013	Herramienta de diagnóstico diligenciada

interior de la Entidad	Herramienta de Diagnóstico del MSPI de MinTic	
Identificar el nivel de madurez de seguridad y privacidad de la información en la entidad	Herramienta de Diagnóstico del MSPI de MinTic	Herramienta de diagnóstico diligenciada
		Establecimiento del nivel de madurez de la entidad frente al MSPI
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Herramienta de Diagnóstico del MSPI de MinTic	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.

8.2. FASE II Planificación

Objetivo: Definir la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad de la información, en procura de los resultados que permitan dar cumplimiento con las metas propuestas.

Tabla 4: Metas de la Planificación

METAS	INSTRUMENTOS O HERRAMIENTAS A UTILIZAR	RESULTADOS ESPERADOS
Política de Seguridad y Privacidad de la Información	Guía No 2 – Política General MSPI	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad
		Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad

Procedimientos de seguridad de la información	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.
Roles y responsabilidades de seguridad y privacidad de la información	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información	Actas de reunion del comité de Historias clínicas y Tics, donde se determinen actividades realizadas sobre temas del manejo y seguridad de la información.
Inventario de activos de información	Guía No 5 - Gestión De Activos.	Inventario de activos de información, conteniendo la identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección
	Guía No 20 - Transición Ipv4 a Ipv6.	Matriz con la identificación, valoración y clasificación de activos de información.
		Documento con la caracterización de activos de información, que contengan datos personales
		Inventario de activos de IPv4 y/o IPv6.
Integración del MSPI con el Sistema de Gestión documental	Guía No 6 - Gestión Documental	Integración del MSPI, con el sistema de gestión documental de la entidad.
Identificación, Valoración y tratamiento de riesgo	Guía No 7 - Gestión de Riesgos. Guía No 8 - Controles de Seguridad	Documento con la metodología de gestión de riesgos.
		Documento con el análisis y evaluación de riesgos.
		Documento con el plan de tratamiento de riesgos.
		Documento con la declaración de aplicabilidad.

		Revisados y aprobados por la alta Dirección
Plan de Comunicaciones	Guía No 14 - Plan de comunicación, sensibilización y capacitación	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.
Plan de diagnóstico de IPv4 a IPv6	Guía No 20 - Transición IPv4 a IPv6	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6

8.3. FASE III Implementación

Objetivo: Llevar acabo la implementación de la fase de planificación del SGSI, teniendo en cuenta para esto los aspectos más relevantes en los procesos de implementación del Sistema de Gestión de Seguridad de la Información de la entidad.

Tabla 5: Metas de la Implementación

METAS	INSTRUMENTOS O HERRAMIENTAS A UTILIZAR	RESULTADOS ESPERADOS
Planificación y Control Operacional	Documento con el plan de tratamiento de riesgos	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta dirección
	Documento con la declaración de aplicabilidad	
Implementación del plan de tratamiento de riesgos	Documento con la declaración de aplicabilidad	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso
	Documento con el plan de tratamiento de riesgos	
Indicadores De Gestión	Guía No 9 - Indicadores de Gestión SI	Documento actualizado de los indicadores de gestión de seguridad y privacidad de la información.
Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6

	IPv6 en la entidad, aprobado por la Oficina de TI	Guía No 20 - Transición de IPv4 a IPv6 para Colombia
		Guía No 19 – Aseguramiento del Protocolo IPv6

8.4. FASE IV Evaluación De Desempeño

Objetivo: Evaluar el desempeño y la eficacia del SGSI, a través de instrumentos que permita determinar la efectividad de la implantación del SGSI.

Tabla 6: Metas de la Evaluación de Desempeño

METAS	INSTRUMENTOS O HERRAMIENTAS A UTILIZAR	RESULTADOS ESPERADOS
Plan de revisión y seguimiento, a la implementación del MSPI	Guía No 16 – Evaluación del desempeño	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección
Plan de Ejecución de Auditorias	Guía No 15 – Guía de Auditoría	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección

8.5. FASE V Mejora Continua

Objetivo: Consolidar los resultados obtenidos del componente 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 SGSI.

Tabla 7: Meta del Mejoramiento Continuo

METAS	INSTRUMENTOS O HERRAMIENTAS A UTILIZAR	RESULTADOS ESPERADOS
Plan de mejora continua	Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI. Guía No 17 – Mejora Continua.	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.

Tabla 8: Cronograma de Desarrollo de Actividades

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CRONOGRAMA DE ACTIVIDADES 2023 - 2024

ACTIVIDADES	GUIA DEL MSPI ASOCIADA	AÑO 1												AÑO 2											
		M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
FASE DE PLANIFICACIÓN (PLANEAR)																									
Integración del MSPI con el Sistema de Gestión Documental.	Guía No. 6	PENDIENTE POR TRD												PENDIENTE POR TRD											
Identificación, valoración y Tratamiento del riesgo.	Guía No. 7 y 8																								
Plan de Comunicaciones.	Guía No. 14													CUMPLIDO											
Plan de diagnóstico de IPv4 a IPv6.	Guía No. 20																								
FASE DE IMPLEMENTACIÓN (HACER)																									
Planificación y control de operacional.																									
Implementación del plan de tratamiento del riesgo.	Guía No. 7																								
Indicadores de gestión.	Guía No. 9																								
Plan de transición de IPv4 a Ipv6.	Guía No. 19 y 20																								
FASE DE EVALUACIÓN DE DESEMPEÑO (VERIFICAR)																									
Plan de revisión y seguimiento, a la implementación del MSPI.	Guía No. 16																								
Plan de Ejecución de auditorias.	Guía No. 15																								
FASE MEJORA CONTINUA (ACTUAR)																									
Plan de mejora continua.	Guía No. 17																								

CONTROL DE CAMBIOS

E: Elaboración del documento.
M: Modificación del documento
X: Eliminación del documento

VERSIÓN	CONTROL DE CAMBIOS AL DOCUMENTO	INFORMACIÓN DE CAMBIOS					ACTO ADMINISTRATIVO/NORMA DE ADOPCIÓN
		E	M	X	Actividades o Justificación	Elaboró / Actualizó	
V-01	Plan de seguridad y privacidad de la información		X		Se modifica el documento por actualización Objetivos, Actividades.	ROBERTO E FREIRE BURBANO	Decreto 612/2018, Ley 1474/2011 Art. 74
V-02	Plan de seguridad y privacidad de la información		X		Se modifica el documento por actualización Objetivos, Actividades.	ROBERTO E FREIRE BURBANO	Decreto 612/2018, Ley 1474/2011 Art. 74
V-03	Plan de seguridad y privacidad de la información		X		Se modifica el documento por actualización en Justificación, definiciones y cronograma de actividades.	ROBERTO E FREIRE BURBANO	Decreto 612/2018, Ley 1474/2011 Art. 74
V-03	Plan de seguridad y privacidad de la información		X		Se modifica por normatividad, se actualiza cronograma.	ROBERTO E FREIRE BURBANO	Decreto 612/2018, Ley 1474/2011 Art. 74

ROBERTO FREIRE BURBANO _____ Realizado por: PROFESIONAL CONTRATISTA GESTIÓN DE LA INFORMACIÓN	HENRY LUIS RODRIGUEZ C. _____ Revisado Por: PROFESIONAL ESPECIALIZADO GESTIÓN DE LA INFORMACIÓN	NILSEN ALVEAR ACOSTA _____ Aprobado por: GERENTE	30-01-2021 Fecha de aprobación