E.S.E. HOSPITAL UNIVERSITARIO SAN RAFAEL DE TUNJA		
CÓDIGO: S-M-08	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	
VERSIÓN: 003		FECHA: 2024-06-12

TABLA DE CONTENIDO

1. INTRODUCCIÓN Y/O JUSTIFICACIÓN

La E.S.E Hospital Universitario San Rafael de Tunja, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Modelo de Seguridad y Privacidad de la Información -MSPI, de acuerdo con la Política de Gobierno Digital y en concordancia con la misión y visión de la entidad, busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado y de los servicios que prestan al ciudadano.

La información tiene la característica de ser uno de los activos más importantes para cualquier organización, debido a que de su tratamiento confidencial depende la rentabilidad y continuidad de su modelo de negocio, por esta razón la seguridad de la información resulta ser un factor crítico para la estabilidad de la entidad.

Mediante la utilización del Modelo de Seguridad y Privacidad para las Entidades del Estado, se busca contribuir al incremento de la transparencia en la gestión pública, promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital; dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en las entidades.

El plan de Seguridad y Privacidad de la Información, tiene como propósito el cumplimiento de los requisitos y lineamientos, que tienen como objetivo, planear y gestionar adecuadamente la seguridad de la información, la gestión de activos, la gestión de riesgos y la continuidad en la prestación de los servicios ofrecidos.

2. OBJETIVO GENERAL

Realizar el plan del seguridad y privacidad de la información para la E.S.E Hospital Universitario San Rafael de Tunja, generando medidas que permitan el aseguramiento y protección de la información de acuerdo a lo exigido en la Política Nacional de Gobierno Digital del Ministerio de las Tecnologías y Comunicaciones -MINTIC.

3. OBJETIVOS ESPECÍFICOS

- Proteger los activos de información de la E.S.E Hospital Universitario San Rafael de Tunja, con base en los principios de confidencialidad, integridad y disponibilidad.
- Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico.

4. ALCANCE

Aplica sobre los requisitos y lineamientos en seguridad y privacidad de la información exigibles a los procesos estratégicos, misionales, de apoyo y de evaluación de la entidad; teniendo en cuenta los procesos que impactan directamente, la consecución de los objetivos misionales, procesos y sistemas de información.

5. MARCO LEGAL APLICABLE

Constitución Política de Colombia de 1991, Articulo 15, consagra que todas las personas tienen el derecho a su intimidad personal y familiar y a su buen nombre. De igual modo, tienen el derecho a conocer, actualizar y a rectificar las informaciones que hayan recogido sobre ellas en los bancos de datos y en los archivos de las entidades públicas y privadas.

Ley 23 de 1982, Ley de propiedad intelectual y derechos de autor.

Ley 527 de 1999, Ley por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación.

Ley 594 de 2000, Ley General de Archivos, la presente ley tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado.

Ley 1266 de 2008, Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Resolución 1995 de 1999, Normas para el Manejo de la Historia Clínica.

Ley 1437 de 2011, Código de procedimiento Administrativo y de lo contencioso administrativo,

Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentada parcialmente en el decreto 1377 de 2013 y en el capítulo 25 del decreto 1074 de 2015,

Decreto 2578 de 2012, Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye “El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles” entre otras disposiciones.

Decreto 2609 de 2012, Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.

Norma técnica colombiana NTC/ISO 27001:2013, Sistema de seguridad de la Información

Norma ISO 27001, Sistemas de Gestión de la Seguridad de la Información.

Ley 1712 DE 2014, Ley de Transparencia y del derecho de acceso a la información pública nacional.

Decreto 1078 de 2015, Decreto único reglamentario del sector de Tecnologías de la Información, por la cual se establece la estrategia de gobierno en línea y dentro de la cual se establece el componente de seguridad y privacidad de la información.

CONPES 3854 de 2016, Política Nacional de Seguridad Digital.

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.

Decreto 1008 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. Tiene como principio la seguridad de la información, que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

6. RESPONSABLE

Lider de seguridad de la información o quien se designe por la Coordinación del proceso de Gestión de la Información y las Comunicaciones de la E.S.E. Hospital Universitario San Rafael de Tunja.

7. RECURSOS, MATERIALES, INSUMOS Y EQUIPOS

- **Humanos:** funcionarios, profesionales y técnicos de TIC.
- **Financieros:** De acuerdo a la disponibilidad asignada para determinada vigencia.
- **Técnicos o recursos tecnológicos**: Computadoras, servidores, teléfonos, sistemas de seguridad, como intangibles sistemas operativos, programas de ciberseguridad, bases de datos, redes internas, entre otros.

8. DESCRIPCIÓN/ IMPLEMENTACIÓN

Dentro de los objetivos especificos del Plan de Gestión 2024-2027 se encuentra el adelantar procesos permanentes de mejoramiento continuo a los procesos de gestión y desarrollo institucional, evaluar y analizar las estrategias que contribuyan al cumplimiento de la misión, visión, objetivos y metas institucionales, con un equipo humano calificado bajo principios y valores enfocados en la prestación de servicios con calidad.

Con la aprobación del Plan de Desarrollo denominado “SAN RAFA, ALMA VIDA Y CORAZON” y en relación al diagnóstico Institucional se realizó la proyección de la misión de la E.S.E. Hospital Universitario San Rafael de Tunja, la cual se en brindar atención en salud integral al paciente y su familia, a través de un talento humano calificado, con enfoque inclusivo, digno y seguro, que contribuye al bienestar y satisfacción de la comunidad, con vocación académica y el mejoramiento continuo.

Este documento se encuentra articulado al Plan de Desarrollo de la Entidad, ya que en este quedo definida la linea estrategica.

- Liderando con Información Para la Salud del Futuro.

Mediante el siguiente objetivo:

- Contribuir al mejoramiento de la gestión de la información para la simplificación de procesos

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Mediante la **Resolución 238 del 08 de junio de 2022** "Por medio de la cual se actualiza la Resolución 050 del 8 de marzo de 2019 y se adopta la Política General de Seguridad y Privacidad de la Información y Seguridad Digital en la E.S.E Hospital Universitario San Rafael de Tunja "

Se compromete con la protección y resguardo de activos de información, bajo los principios de confidencialidad, integridad, disponibilidad de la información; mediante el diagnóstico, planeación, implementación, gestión y mejora continua de un Modelo de Seguridad y Privacidad de la Información, la concientización interna de las políticas en seguridad y privacidad de la información y en concordancia con la Política Nacional de Gobierno Digital, la misión y visión de la entidad.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN -MSPI

Para la implementación del Modelo de seguridad y privacidad de la Información (MSPI), se identificó 5 fases que orientan el ejercicio para los propósitos de protección de la información de la Entidad, bajo un modelo sostenible, propuesto por el Ministerio de las Tecnologías de información – MINTIC.

Las fases del ciclo de operación se definen de la siguiente manera basadas en una fase inicial de diagnóstico:

1. Diagnosticar

2. Planear

3. Implementación

4. Gestión

5. Mejora continua

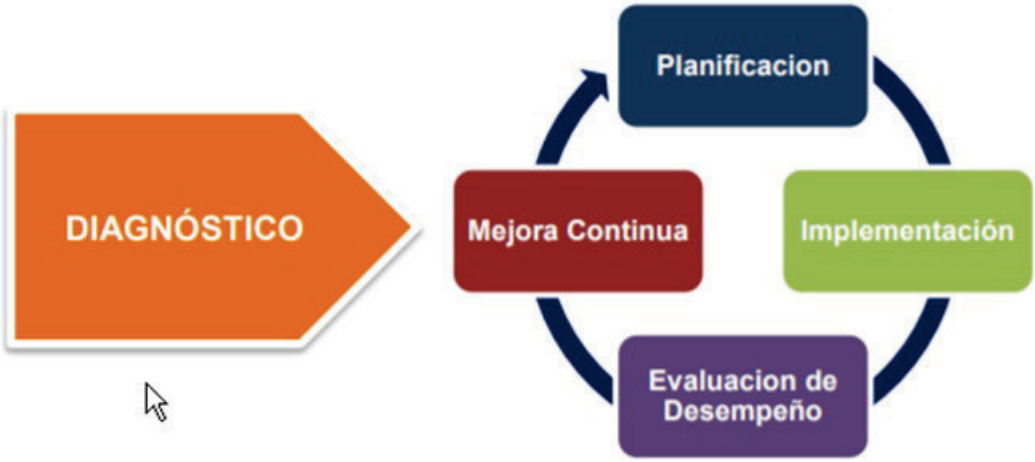


Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

FASE PREVIA DE DIAGNOSTICO DEL MSPI

En esta fase y mediante el uso de herramientas de diagnóstico, se desarrollan actividades de reconocimiento y valoración del estado de gestión, cumplimento de requisitos y lineamientos de seguridad de la información basado con el Modelo de Seguridad y Privacidad de Información de la estrategia de Gobierno Digital del Gobierno Nacional y de la implementación de controles de seguridad de la información con visión de mitigar todo tipo de escenario de riesgo asociado que pudiese generar un impacto indeseado a la entidad.

Figura 2 – Etapas previas a la implementación

Estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad

El diligenciamiento de la herramienta permitió obtener una calificación calculada para cada dominio y está totalizada a partir del valor registrado y promediado sobre la cantidad de objetivos de control que se establecen, todo esto referenciado desde las hojas nombradas como ADMINISTRATIVAS y TÉCNICAS dentro de la Herramienta Instrumento MSPI. El resultado obtenido para la evaluación del estado actual nos refleja los controles y su efectividad según la Normatividad ISO 27001 del 2013 y lo planteado dentro del desarrollo del Modelo de seguridad y privacidad de la información que ha establecido MinTIC para las entidades públicas de orden nacional, así como el avance del ciclo PHVA (Planear-Hacer-Verificar-Actuar). Con el diligenciamiento de la herramienta MSPI, se obtuvieron los siguientes resultados de los dominios para la evaluación y efectividad de controles:

COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Planificación	20%	40%
Implementación	2%	20%
Evaluación de desempeño	0%	20%
Mejora continua	0%	20%
TOTAL	**22%**	**100%**

BRECHA ANEXO A ISO 27001:2013

De acuerdo con la evaluación realizada y el diagnóstico obtenido, la entidad está en un proceso medio con respecto a los aspectos referentes a la implementación de medidas y controles destinados a la privacidad y seguridad de la información así mismo como la protección de los activos que la contienen. La brecha identificada mediante el desarrollo de esta evaluación se puede ver identificada en el siguiente gráfico.

Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad

La madurez de la seguridad y privacidad de la información incluye los controles tanto administrativos como técnicos, la competencia técnica de los recursos informáticos, las directivas, los procesos y las prácticas sostenibles, así como la eficiencia de los controles establecidos dentro de la organización. La madurez de la seguridad se puede medir únicamente a través de la capacidad de la entidad para utilizar de forma eficaz

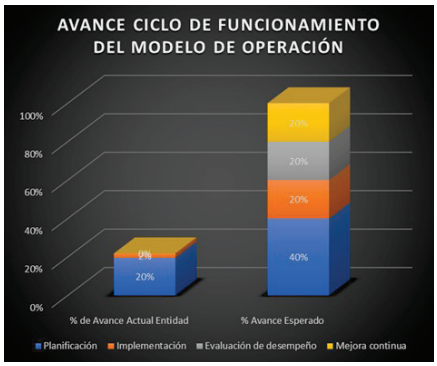
Las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de muchas disciplinas. Para ello debe establecerse una línea de partida de la madurez de la seguridad y usarse para definir las áreas en las que centra los programas de seguridad de la entidad, para el desarrollo del proyecto, el nivel de madurez se identificó mediante el diligenciamiento del Instrumento de Evaluación MSPI evidenciado en la hoja llamada madurez MSPI, que permitió identificar el estado actual y las carencias con las que cuenta la E.S.E Hospital Universitario San Rafael de Tunja, con respecto al Modelo de Seguridad y Privacidad de la Información y se identificaron requisitos que en su mayoría han sido previamente evaluados en las hojas Administrativas, Técnicas y PHVA. En el resultado obtenido al diligenciar la herramienta Instrumento de Evaluación MSPI, el HSRT alcanza el **nivel crítico de madurez** y de cumplimiento de acuerdo con la implementación del Modelo de Seguridad y Privacidad de la Información.

NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

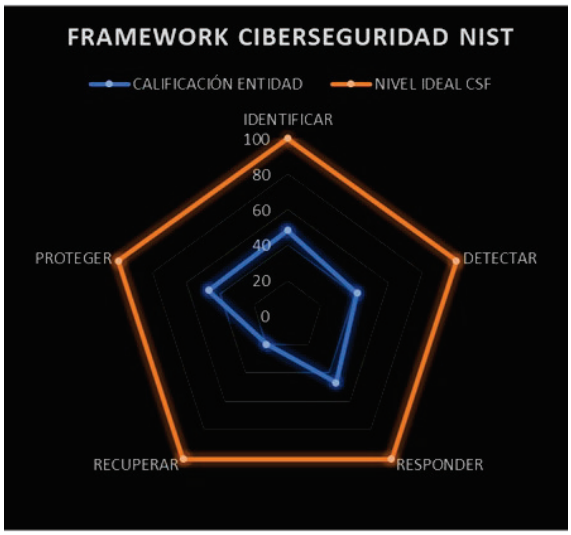
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO		
Inicial	SUFICIENTE	71% a 100%	
Repetible	INTERMEDIO	36% a 70%	
Definido			
Administrado	CRÍTICO	0% a 35%	
Optimizado			
	CALIFICACIONES DE CUMPL		

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.

Según el análisis realizado para la tabla (Tabla 3 - 2 Avance Ciclo de Funcionamiento Del Modelo De Operación (PHVA)), la E.S.E. Hospital Universitario San Rafael de Tunja, se encuentra en un proceso critico de cumplimiento con respecto al PHVA y todo lo referente a la implementación.



MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	**CALIFICACIÓN ENTIDAD**	**NIVEL IDEAL CSF**
IDENTIFICAR	48	100
DETECTAR	41	100
RESPONDER	47	100
RECUPERAR	20	100
PROTEGER	47	100



FASE DE PLANEACION

Para el desarrollo de esta fase y basado en el resultado de la evaluación de diagnóstico y análisis de contexto de la entidad, se identificarán los aspectos claves que definan y orienten las actividades para los propósitos de seguridad y privacidad de la información, entre ellos, el alcance, la política y los objetivos del Modelo de Seguridad y Privacidad de la Información (MSPI).

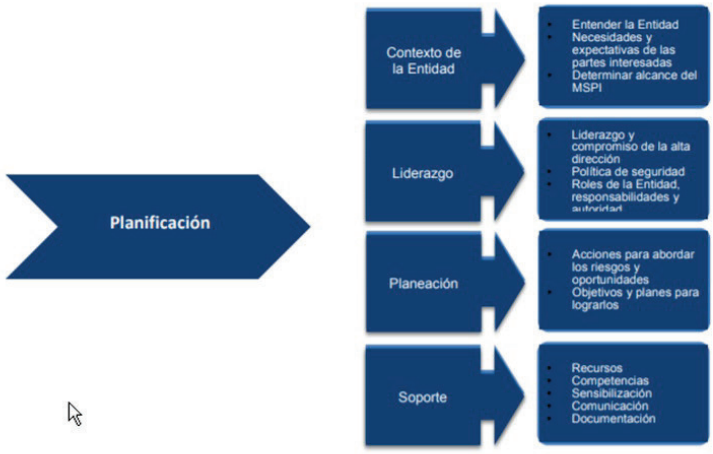


Figura 3 - Fase de planificación[1]

PLANIFICACIÓN		
Metas	**Responsable**	**Resultados**
Política de Seguridad y Privacidad de la Información	Líder de TIC Lider de Seguridad de la Información	**Resolución 238 del 08 de junio de 2022** "Por medio de la cual se actualiza la Resolución 050 del 8 de marzo de 2019 y se adopta la Política General de Seguridad y Privacidad de la Información y Seguridad Digital en la E.S.E Hospital Universitario San Rafael de Tunja " **S-M-02 MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION - V5**
Procedimientos de seguridad de la información.	Líder de TIC Lider de Seguridad de la Información	**S-PR-13 GESTIÓN DE USUARIOS PARA EL ACCESO A SISTEMAS DE INFORMACION Y/O PLATAFORMAS INSTITUCIONALES - V6** **S-PR-21 COPIAS DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN - V4** **S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN - V2** **S-PR-27 CONTINGENCIA ANTE INTERRUPCIONES EVENTUALES EN EL SISTEMA DE INFORMACIÓN SERVINTE CLINICAL SUITE ENTERPRISE. - V1** **S-PR-30 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN - V1** S-F-54 **REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** S-F-55 ACTA DE RECOLECIÓN DE EVIDENCIAS DE INCIDENTES DE SEGURIAD DE LA INFORMACIÓN S-F-56 **NOTIFICACIÓN FINAL DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**
Roles y responsabilidades de seguridad y privacidad de la información.	Líder de TIC Lider de Seguridad de la Información	Resolución 132 de 2024 Por medio de la cual se deroga la Resolución No. 262 de 30 de junio de 2022, que se integra y establece el reglamento de funcionamiento del Comité Institucional de Gestión y Desempeño de la ESE Hospital Universitario San Rafael de Tunja.

Inventario de activos de información	Líder de TIC Lider de Seguridad de la Información	**S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN - V2** **S-INS-21 INSTRUCTIVO DILIGENCIAMIENTO MATRIZ INVENTARIO CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN - V3** **S-M-12 MANUAL METODOLOGÍCO PARA EL LEVANTAMIENTO ACTIVOS DE INFORMACIÓN - V3**
		S-F-46 FORMATO MATRIZ LEVANTAMIENTO ACTIVOS DE INFORMACION - V3
		Documento con la caracterización de activos de información, que contengan datos personales
		PLAN DE DIAGNOSTICO TRANSICION Y ADOPCION DEL PROTOCOLO A IPv6 v3.pdf
Integración del MSPI con el Sistema de Gestión documental	Líder de TIC Lider de Seguridad de la Información	Integración del MSPI, con el sistema de gestión documental de la entidad.
Identificación, valoración y tratamiento de riesgo.	Líder de TIC Lider de Seguridad de la Información	S-M-11 **MANUAL METODOLÓGICO PARA LA GESTIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN** **OADS-F-20 PLAN INSTITUCIONAL/ ESTRATEGICO - V1** **S-F-51 MATRIZ DE RIESGO SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN - MSPI - GOBIERNO DIGITAL E.S.E. HOSPITAL UNIVERSITARIO SAN RAFAEL TUNJA - V4** **S-F-29 DECLARACIÓN DE APLICABILIDAD CONTROLES ISO - V2**
Plan de Comunicaciones.	Líder de TIC Lider de Seguridad de la Información	**CO-PR-04 ELABORACION DEL PLAN DE COMUNICACIONES - V8**
Plan de diagnóstico de IPv4 a IPv6.	Líder DE TIC Lider de Seguridad de la Información	Se cuenta con documento PLAN DE DIAGNÓSTICO PARA LA TRANSICION Y ADOPCION DEL PROTOCOLO IPv6

FASE DE IMPLEMENTACION

El desarrollo de esta fase permitirá a la E.S.E Hospital Universitario San Rafael de Tunja llevar a cabo la implementación de los aspectos y planes identificados en las fases anteriores (diagnóstico y planeación).

Figura 4 - Fase de implementación[2]

Implementación		
Metas	**Responsable**	**Resultados**
Planificación y Control Operacional.	Líder de TIC Lider de Seguridad de la Información Líder de Planeación	**OADS-F-20 PLAN INSTITUCIONAL/ ESTRATEGICO - V1** **S-F-51 MATRIZ DE RIESGO SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN - MSPI - GOBIERNO DIGITAL E.S.E. HOSPITAL UNIVERSITARIO SAN RAFAEL TUNJA - V4** **S-F-29 DECLARACIÓN DE APLICABILIDAD CONTROLES ISO - V2**
Implementación del plan de tratamiento de riesgos.	Líder de TIC Lider de Seguridad de la Información Líder de Planeación	**OADS-F-20 PLAN INSTITUCIONAL/ ESTRATEGICO - V1** **S-F-51 MATRIZ DE RIESGO SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN - MSPI - GOBIERNO DIGITAL E.S.E. HOSPITAL UNIVERSITARIO SAN RAFAEL TUNJA - V4** **S-F-29 DECLARACIÓN DE APLICABILIDAD CONTROLES ISO - V2**
Indicadores De Gestión.	Líder de TIC Lider de Seguridad de la Información Líder de Planeación	Se encuentra en construcción de Fichas Técnicas
Plan de Transición de IPv4 a IPv6	Líder de TIC Lider de Seguridad de la Información	Documento con las PLAN DE IMPLEMENTACION DEL NUEVO PROTOCOLO v2.pdf

ACTIVIDADES PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACÍON

Para la vigencia 2024 se definieron las siguientes actividades :

ACTIVIDAD / ESTRATEGIA	**PRODUCTO**
Actualizar el Plan de Seguridad y privacidad de la información	Documentos S-M-08 plan de seguridad y privacidad de la información.

Actualizar Manual de Políticas de Seguridad y Privacidad de la Información y Seguridad Digital	Manual de Políticas actualizado
Priorizar e Implementar Políticas de Seguridad y Privacidad de la Información y Seguridad Digital	Políticas priorizadas e implementadas
Actualizar el Autodiagnóstico de MSPI herramienta MINTIC.	Documento Autodiagnóstico MINTIC.
Elaborar curso virtual de Seguridad y Privacidad de la Información y Seguridad Digital	Curso virtual
Actualizar el formato S-F-29 Diagnóstico Controles Del SGSI -ISO/IEC 27002:2013 " ISO/IEC 27002:2013. 14 Dominios, 35 Objetivos De Control Y 114 Controles "Modelo De Seguridad Y Privacidad De La Información - MSPI	Formato S-F-29 actualizado
Presentar Resultados en el comité de gestión y desempeño institucional	Acta Comité Gestión y Desempeño Institucional

GESTION Y EVALUACIÓN DESEMPEÑO DEL MSPI

Con el propósito de conocer los estados de cumplimiento de los objetivos de seguridad de la información, se mantendrán esquemas de seguimiento y medición al cumplimiento de aspectos del modelo de seguridad y privacidad de información que permitan contextualizar una toma de decisiones de manera oportuna.

El proceso de seguimiento y monitoreo del Modelo de Seguridad y Privacidad de la Información -MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Figura 5 - Fase de Evaluación de desempeño[3]

EVALUACIÓN

Se realizará seguimiento y evaluación a través del seguimiento a los formatos:

- **OADS-F-20 PLAN INSTITUCIONAL/ ESTRATEGICO - V1**
- **S-F-29 DECLARACIÓN DE APLICABILIDAD CONTROLES ISO - V2**
- Herramienta de Diagnostico MSPI -MINTIC

MANTENIMIENTO Y MEJORA CONTINUA DEL MSPI

En esta fase la Entidad debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

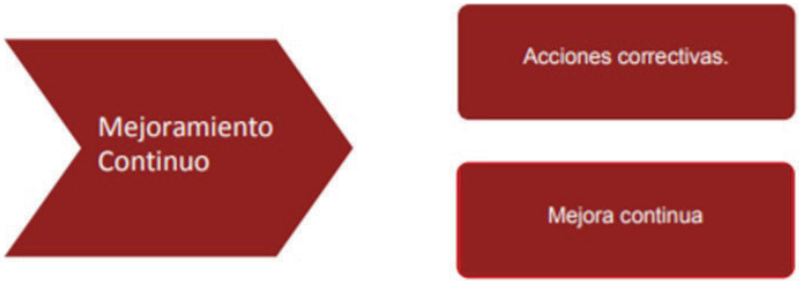


Figura 6 - Fase de mejoramiento continúo[4]

- Implementará las mejoras identificadas en el Modelo de Seguridad y Privacidad de la Información- MSPI.
- Identificará e implementará acciones correctivas y preventivas que mitiguen situaciones de impacto.
- Implementará acciones de mejora basadas en las lecciones aprendidas de las experiencias de seguridad internas o de otras compañías.
- Asegurar que las mejoras cumplen con los objetivos y propósitos definidos por la gerencia de la ESE Hospital Universitario San Rafael de Tunja.

10. DEFINICIONES Y/O GLOSARIO

Activo de Información. Recurso tangible e intangible del o de los sistemas de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Entendiendo por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la entidad.

Análisis del riesgo. Uso sistemático de la información para identificar las fuentes y calcular el riesgo.

Amenaza. Son los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos de información, puede ser de dos tipos: Amenazas internas y Amenazas externas.

Control. Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

Diagnóstico. es el análisis que se realiza para determinar cualquier situación y cuáles son las tendencias. Esta determinación se realiza sobre la base de datos y hechos recogidos y ordenados sistemáticamente, que permiten juzgar mejor qué es lo que está pasando.

Evaluación del riesgo. Proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo.

Evaluación de la Amenaza. es el proceso mediante el cual se determina la probabilidad de ocurrencia y la severidad de un evento en un tiempo específico y en un área determinada. Representa la ocurrencia estimada y la ubicación geográfica de eventos probables.

Evento de seguridad de la información. Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida.

Gestión del riesgo. Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

Incidentes de seguridad de la información. Procesos para detectar, reportar, evaluar, responder, tratar y gestionar los fallos de seguridad de la información. (ISO/IEC 27000).

Información. Conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Impacto. Es la consecuencia negativa sobre un activo de la materialización de una amenaza.

Incidente de seguridad de la información. Evento que atenta contra la confidencialidad, integridad o disponibilidad de la información y los recursos tecnológicos. Evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

Lineamiento. Una descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos.

MSPI. Modelo de Seguridad y privacidad de la Información por sus siglas MSPI, dispuesto a aplicar por las entidades del estado en el marco De la Política de Gobierno Digital.

Normas ISO 27000. El estándar ISO 27000 apunta a exigir niveles concretos y adecuados de seguridad informática, niveles necesarios para las empresas que compiten a través del comercio electrónico y que por lo tanto tienen que exponer sus infraestructuras de información.

Política. Intención y dirección general expresada formalmente por la gerencia.

Confidencialidad. Es la propiedad de la información, por la que se gestiona que es accesible únicamente a personal autorizado a conocer la información.

Integridad. Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.

Disponibilidad. Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

SGSI: Sistema de Gestión de la Seguridad de la Información, es utilizada para referirse a la gestión de los procesos y mecanismos de control que son utilizados para custodiar y proteger de amenazas la información sensible de las organizaciones. Los SGSI permiten a la gerencia de las organizaciones determinar con objetividad que información requiere ser protegida, por qué debe ser protegida, de qué debe ser protegida y como protegerla mediante la planificación e implantación de políticas, procedimientos y controles que mantengan siempre el riesgo por debajo del nivel asumible por la propia organización.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

Vulnerabilidad: debilidad de un activo que puede ser aprovechada por una amenaza.

11. DOCUMENTO SOPORTE /ANEXOS

S-M-02 MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION - V5

S-PR-13 GESTIÓN DE USUARIOS PARA EL ACCESO A SISTEMAS DE INFORMACION Y/O PLATAFORMAS INSTITUCIONALES - V6

S-PR-21 COPIAS DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN - V4

S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN - V2

S-PR-27 CONTINGENCIA ANTE INTERRUPCIONES EVENTUALES EN EL SISTEMA DE INFORMACIÓN SERVINTE CLINICAL SUITE ENTERPRISE. - V1

S-PR-30 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN - V1

S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN - V2

S-INS-21 INSTRUCTIVO DILIGENCIAMIENTO MATRIZ INVENTARIO CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN - V3

S-M-12 MANUAL METODOLOGÍCO PARA EL LEVANTAMIENTO ACTIVOS DE INFORMACIÓN - V3

S-F-46 FORMATO MATRIZ LEVANTAMIENTO ACTIVOS DE INFORMACION - V3

S-M-11 **MANUAL METODOLÓGICO PARA LA GESTIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN**

OADS-F-20 PLAN INSTITUCIONAL/ ESTRATEGICO - V1

S-F-51 MATRIZ DE RIESGO SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN - MSPI - GOBIERNO DIGITAL E.S.E. HOSPITAL UNIVERSITARIO SAN RAFAEL TUNJA - V4

S-F-29 DECLARACIÓN DE APLICABILIDAD CONTROLES ISO - V2

Herramienta de Diagnostico MSPI -MINTIC

12. SOPORTE /ANEXOS

No Aplica

13. BIBLIOGRAFÍA

Procedimientos De Seguridad de La Información

https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

Guía para la Gestión y Clasificación de Activos de Información

http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Modelo de Seguridad y Privacidad de la Información

http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

CONTROL DE CAMBIOS			
VERSIÓN	**FECHA**	**ELABORÓ**	**DESCRIPCIÓN DEL CAMBIO**
1	20/12/2018	Alfredo Orjuela Peña	Versión Original
2	30/11/2023	Jorge Armando Figueredo Malagon	Se ajustan siglas de TICS a TIC y ESE a E.S.E
3	19/06/2024	Jorge Armando Figueredo Malagon- Erika Ortiz- Karenth Jimenez	Se relaciona documentos con los que cuenta la entidad en cada una de las fases del ciclo de operación de seguridad. Se incluye actividades del plan de seguridad y privacidad de la información para la vigencia Se anexan documentos soportes/anexos.

Elaboró	Revisión Técnica	Socialización	Revisión General	Aprobó
Nombre: Marbiz Said Ducuara Amado Cargo: Profesional Universitario	Marbiz Said Ducuara Amado Profesional Universitario Blanca Nelly Castiblanco Sierra Apoyo a Gestión por Procesos	Blanca Nelly Castiblanco Sierra Apoyo a Gestión por Procesos Karenth Paola Jimenez Santamaria Profesional Especializado	Monica Maria Londoño Forero Asesor Desarrollo de Servicios	German Francisco Pertuz Gonzalez Gerente