PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Hospital San Rafael, Empresa Social del estado

Municipio de El Águila, Valle del Cauca

Vigencia 2023.

Tabla de contenido

1. Introducción 3
2. Objetivos 4
2.1. General 4
2.2. Objetivo específico 4
3. Términos y definiciones.....4
4. Marco Normativo 5
5. Situación actual 6
6. Actividades a desarrollar en el año 2023. 8

1. Introducción.

El presente documento describe el Plan de Seguridad y Privacidad del Hospital San Rafael, Empresa Social del Estado, alineado con los objetivos, metas, procesos, procedimientos y estructura organizacional. Las entidades públicas están cada vez más expuestas a sufrir incidentes de seguridad digital, lo cual, puede afectar su funcionamiento repercutiendo en la prestación de los servicios a la ciudadanía.

El MinTIC elaboró el Modelo de Seguridad y Privacidad de la Información – MSPI y define los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de los sujetos obligados un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten que las Entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información. Por ello, los sujetos obligados deben abordar las siguientes fases:

1. **Diagnóstico:** Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.
2. **Planificación:** Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.
3. **Operación:** Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.
4. **Evaluación de desempeño:** Determinar el sistema y forma de evaluación de la adopción del modelo.
5. **Mejoramiento Continuo:** Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

Cada una de las fases se dará por completada, cuando se cumplan todos los requisitos definidos en cada una de ellas.

2. OBJETIVOS

2.1. Objetivo general.

Describir las actividades del plan de Seguridad y Privacidad de la Información, con las cuales se busca desarrollar, verificar y aplicar la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI del Hospital San Rafael, Empresa Social del Estado, del municipio de El Águila.

2.2. Objetivos específicos.

- Implementar, Proteger los activos de información del Hospital San Rafael E.S.E, con base en los criterios de confidencialidad, integridad y disponibilidad.
- Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
- Sensibilizar a los servidores públicos y contratistas de la Entidad acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la Entidad.
- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico.
- Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información de Gobierno Digital".

3. TÉRMINOS Y DEFINICIONES.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad[1].

Seguridad de la Información: Este principio 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.

4. MARCO NORMATIVO.

MARCO NORMATIVO	DESCRIPCIÓN
Decreto 103 de 2015.	Compendio de políticas aplican para todos los servidores públicos y contratistas del Hospital San Rafael E.S.E. que procesan y/o manejan información de la entidad.
Decreto 1494 de 2015.	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1008 de 2018.	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Ley 1712 de 2014.	Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
Decreto 2573 de 2014.	Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones.
Decreto 1377 de 2013.	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 2609 de 2012.	Por el cual se reglamenta parcialmente la Ley 1581de 2012.
Ley estatutaria 1581 de 2012.	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.

[1] Decreto 1008 del 14 de junio del 2018, por el cual se establecen los lineamientos generales de la Política de Gobierno Digital.

Ley 1474 de 2011.	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Decreto 4632 de 2011.	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Ley 1273 de 2009.	Se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
Ley 527 de 1999.	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.
Constitución Política de Colombia1991 - Artículo 15.	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.
Ley 23 de 1982.	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.
Norma técnica colombiana NTC - ISO/IEC 27001.	Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa.
Ley 1581 de 2012.	Por la cual se dictan disposiciones generales para la protección de datos personales.

5. SITUACIÓN ACTUAL.

El Hospital San Rafael E.S.E. ha realizado actividades tendientes a la adopción del Modelo de Seguridad y Privacidad de la Información, para lo cual se consultó la normatividad, guías, planes, la política y manual Seguridad y Privacidad de la Información, obteniendo los siguientes resultados:

ÁMBITO	SITUACIÓN ACTUAL
	No se cuenta con un diagnóstico que contenga el estado de la implementación del modelo de Seguridad y Privacidad de la

Diagnóstico de seguridad y privacidad.	Información del Hospital San Rafael E.S.E. Se debe realizar el diagnostico relacionado con la Seguridad y Privacidad de la Información.
Plan de Seguridad y Privacidad.	En la vigencia 2022, se crea y formaliza el plan de seguridad y privacidad de la información para la vigencia 2022 y se actualiza en la vigencia 2023. Así mismo, se tiene proyectado dentro del plan las actividades a realizar en la vigencia 2023. Es necesario fortalecer los procesos y procedimientos que hacen referencia a la implementación de la seguridad y privacidad de la información de la entidad. La entidad debe definir los riesgos de seguridad para cada uno de los procesos de la entidad y llevar el control de la ejecución de las acciones preventivas asociadas en el Sistema de Gestión Institucional (actividades, tiempos y responsables). Se debe definir los riesgos y controles con los delegados de cada proceso.
Plan de Implementación.	El plan de seguridad y privacidad de la información, se actualizará periódicamente con el fin de hacer seguimiento a las acciones definidas en cada vigencia y determinar las acciones a realizar en las siguientes vigencias como también se deberá mantener actualizada la declaración de aplicabilidad de la seguridad de la información. Se deberá asignar el área encargada de la identificación de riesgos e implementación de controles de

	Seguridad y Privacidad de la Información.
Gestión de Riesgos.	El hospital San Rafael E.S.E. implementará el manejo y respuesta a incidentes asociados a Seguridad y Privacidad de la Información, mediante el procedimiento denominado Gestión de Incidentes de Seguridad de la Información. Con el fin de garantizar la transferencia segura de datos de carácter personal requeridos por los entes de control y vigilancia en el marco de sus funciones misionales, la entidad deberá implementar el procedimiento "Intercambio Seguro de Datos con Entidades de Vigilancia y Control".

6. ACTIVIDADES A DESARROLLAR EN EL AÑO 2023.

Las principales actividades que se desarrollarán en el año 2023, serán las siguientes:

EJE	ÁREA	ACTIVIDADES A REALIZAR
Transformación Digital.	Transferencia de información.	Se identificarán riesgos de seguridad digital y se diseñarán los controles de seguridad necesarios para garantizar la seguridad digital y la protección de los datos personales en el marco de los acuerdos de intercambio de información de la entidad con otros.
	Seguridad para los Servicios ciudadanos digitales (sistemas digitales).	Se creará el manual de seguridad de la información para la protección de los datos personales en sistemas de información que realicen tratamiento de datos personales.

Riesgos.	Analizar el panorama de riesgos de seguridad digital.	Acompañamiento a los procesos institucionales en la identificación, valoración, evaluación y formulación de planes de tratamiento de riesgo de seguridad digital.
	Implementación de planes de tratamiento de riesgos.	Acompañamiento a la implementación de los planes de tratamiento de riesgos de seguridad digital que adopten los procesos.
Sensibilización.	Inducción a funcionarios.	Apoyar actividades de inducción de los funcionarios de la entidad con charlas en materia de seguridad de la información, protección de datos personales y controles del sistema de gestión de seguridad de la información.
	Divulgación de la documentación, controles y herramientas de ayuda del sistema de gestión de seguridad de la información.	Diseñar e implementar acciones de socialización de la documentación, controles y herramientas del sistema de gestión de seguridad de la información institucional.
	Continuidad de la plataforma tecnológica y de servicios.	Apoyar técnicamente la implementación de soluciones de detección de intrusos que protejan la infraestructura de servicios institucionales.
		Apoyar técnicamente la implementación de soluciones de protección perimetral de los sistemas de información ante ataques cibernéticos.
		Acompañar el diseño de lineamientos y controles de seguridad que

		mitiguen los riesgos que puedan impactar la infraestructura de servicios de nube privada institucional
Sistema integrado de planeación y gestión.	Gestión de la Documentación del Sistema de gestión de seguridad de la información.	Diseñar estrategias y controles que permitan la implementación de las políticas de seguridad de la información en los procesos institucionales.
		Elaborar los documentos del sistema de gestión de seguridad de la información requeridos por la Norma ISO 27001 y el modelo de seguridad y privacidad de la Información recomendado por el Ministerio de las Tecnologías de la Información y las Comunicaciones.
	Medición del desempeño	Realizar la evaluación de la efectividad de los controles de seguridad de la información adoptados por la Entidad para el tratamiento de los riesgos de seguridad Digital.
Seguridad operativa.	Gestión de eventos e incidentes de seguridad.	Acompañar a al funcionario encargado de las Tecnologías de información y las comunicaciones en la gestión, evaluación e implementación de acciones de respuesta frente a eventos e incidentes de seguridad de la información.
	Seguridad de la Documentación generada en los procesos.	Apoyar técnicamente la elaboración de lineamientos y controles para mejorar la seguridad

		de los datos procesados en los procesos institucionales a través de sistemas de información.
	Seguridad de Aplicaciones de procesamiento de información de las plataformas estratégicas.	Apoyar el diseño y adopción de procedimientos de protección de datos personales para los procesos institucionales y sistemas de información misionales que realicen tratamiento de datos personales.
	Análisis de vulnerabilidades de plataforma tecnológica.	Realizar análisis de vulnerabilidades sobre los componentes de infraestructura tecnológica y de servicios de la Entidad.
	Ingeniería social.	Apoyar el desarrollo de pruebas de ingeniería social para evaluar el nivel de conciencia en seguridad de la información de los funcionarios, contratistas y colaboradores de la Entidad.

ias S.

CARLOS ARTURO PATIAS SALAZAR
Gerente ESE