	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código	PL_03_SI-2
		Versión	1
		Página	1 de 7


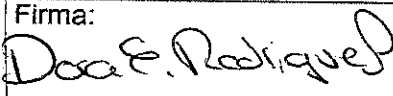

1. JUSTIFICACIÓN


El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, 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 más participativo, más eficiente y más transparente.

La planificación e implementación de la Seguridad y Privacidad de la Información, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad. El Modelo de Seguridad y Privacidad de la Información, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de las estrategias de las empresas del estado. Para el desarrollo del componente de Seguridad y Privacidad de la Información, se ha elaborado un conjunto de documentos asociados al Modelo de Seguridad y Privacidad de la Información, los cuales, a lo largo de los últimos años, han sido utilizados por las diferentes entidades tanto del orden nacional como territorial, para mejorar sus estándares de seguridad de la información. El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; así mismo recoge además de los cambios

Elaboró: Lina María Castaño Responsable SGSST	Revisó: Dora Elena Rodríguez A. Profesional de Calidad	Aprobó: Carlos Fredy Carmona R. Gerente
Firma: 	Firma: 	Firma: 
Fecha: 2018-07-06	Fecha: 2018-07-09	Fecha: 2018-07-10

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código	PL_03_SI-2
		Versión	1
		Página	2 de 7

técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública.


2. OBJETIVOS

2.1 OBJETIVO GENERAL

Generar un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para la E.S.E Hospital San Rafael de Itagüí.

2.2 OBJETIVOS ESPECÍFICOS

- Buscar mediante la utilización de las buenas prácticas de Seguridad y Privacidad 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.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Orientar a las entidades en las mejores prácticas en seguridad y privacidad.
- Optimizar la gestión de la seguridad de la información al interior de la E.S.E Hospital San Rafael de Itagüí.
- Adopción de la legislación relacionada con la protección de datos personales.
- Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones.

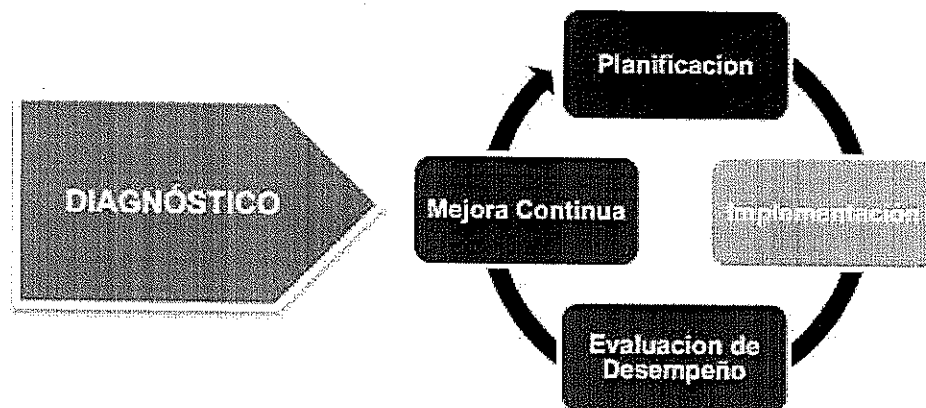
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código	PL_03_SI-2
		Versión	1
		Página	3 de 7


3. ALCANCE

Este plan, proporciona la metodología establecida por la E.S.E Hospital SAN RAFAEL DE ITAGUI para la seguridad y privacidad de la información de todos los procesos; orientando sobre las actividades a desarrollar para velar por la protección de la misma.

4. DESCRIPCIÓN DEL CICLO DE OPERACIÓN

En el presente capítulo se explica el ciclo de funcionamiento de operación, a través de la descripción detallada de cada una de las cinco (5) fases que lo comprenden. Estas, contienen objetivos, metas y herramientas que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de la E.S.E HOSPITAL SAN RAFAEL DE ITAGUI.



	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código	PL_03_SI-2
		Versión	1
		Página	4 de 7

5. PROGRAMACIÓN DE ESTRATEGIAS Y ACTIVIDADES


ESTRATEGIAS	ACTIVIDADES	RESPONSABLES	PLAZOS	MEDIOS DE VERIFICACIÓN
1. FASE DIAGNÓSTICO				
Controles de seguridad establecidos para protección de la información y su nivel de madurez	Realizar un listado de los controles establecidos para proteger toda la información del hospital	Área de tecnología y sistemas	Agosto 2018	Verificación por parte del área de Calidad
Cumplimiento de la legislación de Habeas Data	Verificación de los controles de Habeas Data	Persona responsable de Habeas Data	Agosto 2018	Verificación por parte del área de Calidad
Identificar posibles buenas practicas tecnológicas y de sistemas para a protección y seguridad de la información.	Identificación de posibles prácticas que se podrían implementar para la protección y privacidad de la información	Área de tecnología y sistemas	Agosto 2018	Verificación por parte del área de Calidad
2. FASE DE PLANIFICACIÓN				
Establecer necesidades y expectativas de las partes interesadas con respecto a los controles para la seguridad y privacidad de la información	Realizar análisis de contexto del hospital para identificar las necesidades y expectativas	Área de tecnología y sistemas	Septiembre 2018	Revisión de la información establecida.
Liderazgo	Establecer la política de seguridad y privacidad de la información Roles Responsabilidades	Área de tecnología y sistemas	Septiembre 2018	Aprobación por parte de Gerencia



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Código	PL_03_SI-2
Versión	1
Página	5 de 7

ESTRATEGIAS	ACTIVIDADES	RESPONSABLES	PLAZOS	MEDIOS DE VERIFICACIÓN
Identificar riesgos relacionados con la seguridad y privacidad de la información	Establecer el plan de riesgos de seguridad y privacidad de la información	Área de tecnología y sistemas	Julio 2018	Revisión por parte del área de calidad
Asignación de Recursos	Establecer los recursos necesarios para dar soporte tecnológico y de sistemas para lograr los objetivos	Área de tecnología y sistemas Gerencia	Septiembre 2018	Verificación de la información por parte del área de calidad
Documentar todos los procedimientos y controles para garantizar la seguridad y privacidad de la información	Documentar los controles y actividades que se realizarán para garantizar la seguridad y privacidad de la información.	Área de tecnología y sistemas	Octubre 2018	Verificación de la información por parte del área de calidad
Inventario de activos de la información	Documento con la caracterización de activos de información	Área de tecnología y sistemas Líderes de todas las áreas	Octubre 2018	Verificación con cada líder
3. FASE DE IMPLEMENTACIÓN				
Control operacional frente a los riesgos	Realizar documento con el plan para el tratamiento de los riesgos establecidos Asociar los riesgos con el cumplimiento legal	Área de tecnología y sistemas	Octubre 2018	Verificación de la información por parte del área de calidad
Indicadores de gestión	Documento con la descripción de los indicadores de gestión de seguridad y	Área de tecnología y sistemas	Octubre 2018	Se medirán los casos que se presenten de incumplimiento relacionados.


	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código	PL_03_SI-2
		Versión	1
		Página	6 de 7

ESTRATEGIAS	ACTIVIDADES	RESPONSABLES	PLAZOS	MEDIOS DE VERIFICACIÓN
	privacidad de la información.			
4. FASE DE EVALUACIÓN DE DESEMPEÑO				
Revisión y seguimiento a la implementación	Realizar periódicamente auditoria al cumplimiento	Gerencia Área de Calidad	Noviembre 2018	Auditoria Seguimiento a planes
Plan de ejecución de auditorias	Integrar al plan general de auditorías de la E.S.E, la revisión de el plan de seguridad y privacidad de la información	Área de Calidad	Noviembre 2018	Auditoria
5. FASE MEJORA CONTINUA				
Plan de mejora continua	Documentar plan de mejoramiento de acuerdo a las revisiones periódicas a los requisitos Comunicar los resultados	Área de tecnología y sistemas Área de Calidad	Diciembre 2018	Auditoria

6. METAS

La verificación del cumplimiento de este plan, se realizará por medio de los indicadores de gestión y los resultados de la auditoria y revisión por la dirección.

INDICADOR	META	RESPONSABLE
Número de casos reportados relacionados con la seguridad y la privacidad de la información.	Cero casos	Área de tecnología y sistemas

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código	PL_03_SI-2
		Versión	1
		Página	7 de 7

Cumplimiento de todos los controles tecnológicos para proteger la seguridad y privacidad de la información	100% cumplir los controles tecnológicos	Área de tecnología y sistemas
--	---	-------------------------------

CAMBIOS (*)

FECHA	NATURALEZA DEL CAMBIO	SOLICITANTE

COPIA CONTROLADA