PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

DIEGO LEÓN MUÑOZ ZAPATA

GERENTE

2021

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La E.S.E Hospital San Rafael de Itagüí, en busca de la mejora continua implementa un método lógico y sistemático que permita identificar, analizar, evaluar, tratar, controlar y comunicar la seguridad y Privacidad de la información, para lograr que estos no afecten de una manera relevante los procesos y actividades de la entidad.

La Entidad utiliza Las Tecnologías de la Información y la Comunicación (**TIC**). Para apoyar el cumplimiento de sus metas, en cuanto al ingreso, procesamiento y reporte de información y comunicarse con los diferentes actores del sistema de salud. Implica que sea necesario la seguridad y privacidad de la información, en los procesos Estratégicos, Operativos, Financieros, y Tecnológicos, por lo cual este documento busca establecer una línea de trabajo que permita que su información está segura.

Además, para dar cumplimiento al Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, que es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la Información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en el mapa de procesos, mediante una gestión Integral de riesgos y la implementación de controles físicos y digitales, previniendo así Incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación

masiva de las TIC, a través de políticas y programas, para mejorar la calidad de vida de cada colombiano y el incremento sostenible del desarrollo del país.

2. DOCUMENTOS DE REFERENCIA

- **Constitución Política de Colombia**. Artículo 15.
- **Ley 44 de 1993**. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- **Ley 527 de 1999**. Por 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 y se dictan otras disposiciones.
- **Ley 594 de 2000**. Por medio de la cual se expide la Ley General de Archivos.
- **Ley 850 de 2003**. Por medio de la cual se reglamentan las veedurías ciudadanas.
- **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.
- **Ley 1221 del 2008**. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- **Ley 1273 de 2009**. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1341 de 2009**. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
- **Ley 1437 de 2011**. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- **Ley 1474 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 1581 de 2012**. Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1712 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.
- **Ley 1915 de 2018**. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

- **Ley 1952 de 2019**. Por medio de la cual se expide el código general disciplinario.
- **Ley 1955 de 2019**. por el cual se expide el Plan Nacional de Desarrollo 2018-2122. “Pacto por Colombia, Pacto por la Equidad”.

- **Ley 1978 de 2019**. Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.
- **Decreto 2609 de 2012**. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- **Decreto 0884 del 2012**. Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
- **Decreto 1377 de 2013**. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Decreto 886 de 2014**. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **Decreto 103 de 2015**. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Decreto 1074 de 2015**. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- **Decreto 1078 de 2015**. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1080 de 2015**. Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
- **Decreto 1081 de 2015**. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- **Decreto 728 de 2017**. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
- **Decreto 1499 de 2017**. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- **Decreto 1008 del 2018**. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2

del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

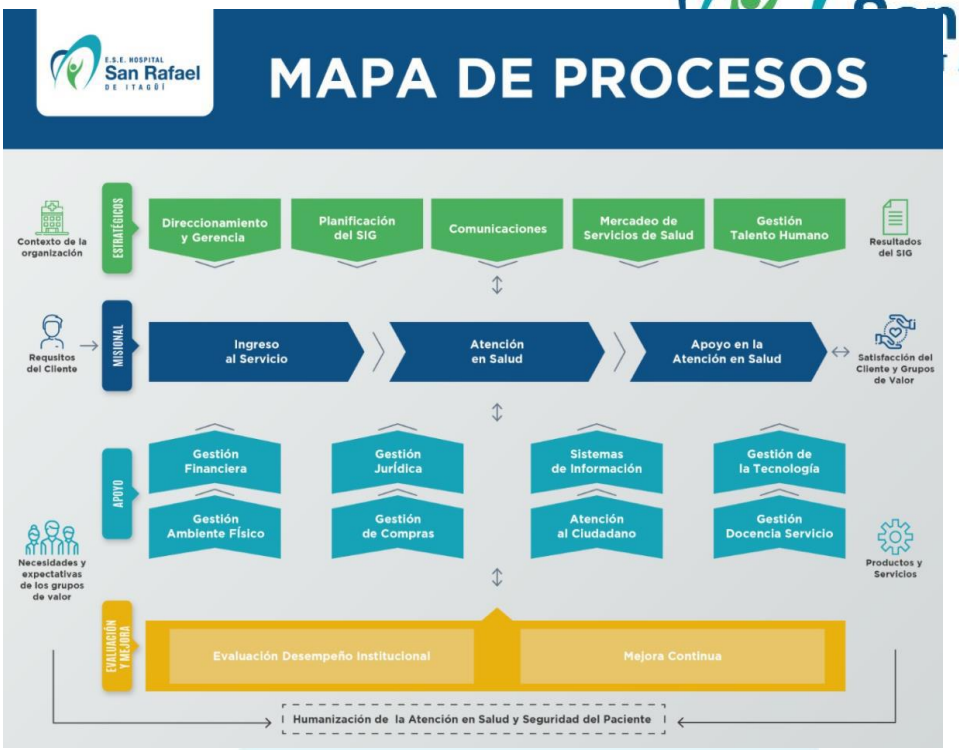
- **Decreto 2106 de 2019**. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- **Decreto 620 de 2020**. por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- **Decreto 1064 de 2020**. Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones
- **Resolución 2999 del 2008**. Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.
- **Resolución 2034 de 2016**. Por la cual se adoptó el Modelo de Responsabilidad Social Institucional en el Ministerio TIC.
- **Resolución 2306 de 2020**. Por la cual se actualiza el Modelo Integrado de Gestión (MIG) del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 911 de 2018.
- **Resolución 1151 de 2019**. Por la cual se establecen las condiciones especiales del Teletrabajo en el Ministerio de Tecnologías de la Información y las Comunicaciones, y se deroga la Resolución 0002133 del 3 de agosto de 2018.
- **Resolución 924 de 2020**. Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo Único de TIC y se deroga la resolución 2007 de 2018.
- **Resolución 2256 de 2020**. Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 1124 de 2020.
- **CONPES 3701 de 2011**. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016**. Política Nacional de Seguridad digital.
- **CONPES 3905 de 2020**. Política Nacional de Confianza y Seguridad Digital.

3. OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio y el Mapa de Procesos de la E.S.E Hospital San Rafael de Itagüí.

4. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Entidad debe Generar conciencia para el cambio organizacional requerido para la apropiación de la Seguridad y Privacidad de la Información, las Políticas Específicas De Manejo De Información, que se dan en cada uno de los procesos, lo cual se deben tener las siguientes Políticas:



- Políticas Específicas De Manejo De Información.
- Política De Seguridad De Los Recursos Humanos.
- Política De Gestión De Activos.
- Política De Control De Acceso.
- Política De Criptografía.
- Política De Seguridad Física Y Del Entorno.
- Política De Seguridad De Las Operaciones.
- Política De Seguridad De Las Comunicaciones.
- Política De Seguridad Para La Adquisición, Desarrollo Y Mantenimiento De Sistemas.
- Política De Seguridad Para Relación Con Proveedores.
- Política De Gestión De Incidentes De Seguridad De La Información.
- Política De La Continuidad Del Servicio.

- Política De Cumplimiento.

3.1 OBJETIVOS ESPECIFICOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN TIC

- Definir los lineamientos para la implementación de mejores prácticas de seguridad que permita identificar las infraestructuras críticas en las entidades.
- Generar buenas prácticas en Seguridad y Privacidad de la información de la E.S.E Hospital San Rafael de Itagüí, que este alineado con Seguridad Digital y Continuidad del Servicio.
- Promover y fortalecer el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital y transparencia en la gestión pública.
- Mitigar los Incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.

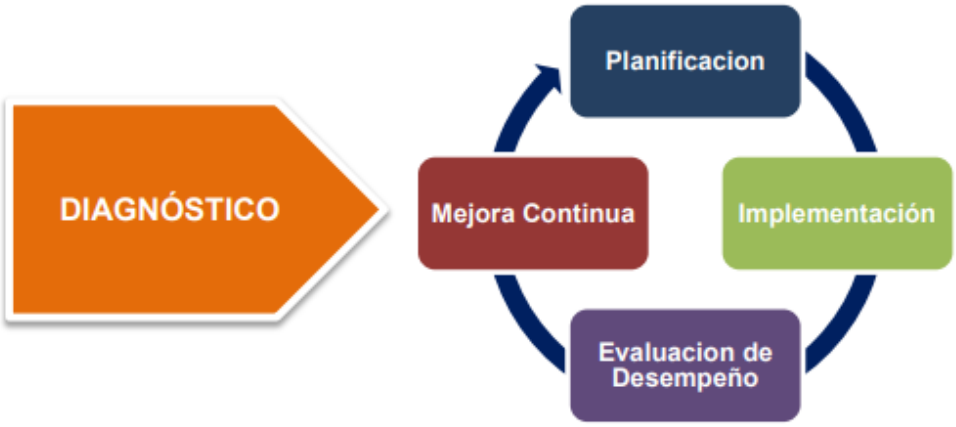
- Generar conciencia para el cambio organizacional requerido para la apropiación de la Seguridad y Privacidad de la Información como eje transversal de la Entidad.

5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Este plan, facilita la metodología establecida por la E.S.E Hospital San Rafael de Itagüí, para la seguridad y privacidad de la información de todos los procesos; para velar por la protección de la información de la Entidad.

Aplica a todos sus funcionarios, Entes de Control, contratistas, proveedores, agremiados y aquellas personas o terceros que debido al cumplimiento de sus funciones compartan, utilicen, recolecten, procesen, intercambien o consulten la información de la Entidad

6. OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI



PLANEAR:

Planificación, Diseño, Sistematización de las políticas a aplicar para alcanzar los objetivos de la E.S.E Hospital San Rafael de Itagüí.

IMPLEMENTAR:

Implementación de las políticas, elaboración de controles y asignación de responsabilidades de cada actividad.

EVALUACIÓN DEL DESEMPEÑO:

Monitorear, revisión del SGSI, Control de Eficaz y eficiente y medición de objetivos

MAJORA CONTINUA:

Acciones preventivas y Correctivas, aplicar auditorias internas, revisión de SGSI.

7. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan de implementación para la dimensión de Seguridad y Privacidad de la información comprende el siguiente cronograma y se le hace seguimiento mes a mes

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE DE LA TAREA	FECHA INICIO	FECHA FINAL
Planeación	Revisión de los documentos de las Políticas	Actualización de los documentos de las Políticas	Área de sistemas	01/01/2021	31/03/2021
		Informe cumplimiento de las políticas	Área de sistemas	01/04/2021	30/11/2021

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE DE LA TAREA	FECHA INICIO	FECHA FINAL
Activos de Información	Lineamientos para el levantamiento de activos de información	Actualización de metodología e instrumento de levantamiento de activos de información.	Área de sistemas Líder de activos Fijos	01/02/2021	30/06/2021
	Levantamiento Activos de Información	Validar activos de información en el instrumento levantado en la vigencia anterior	Área de sistemas Líder de activos Fijos	01/02/2021	30/06/2021
		Identificar nuevos activos de información en cada dependencia	Área de sistemas Líder de activos Fijos	01/02/2021	30/06/2021

		Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información	Área de sistemas Líder de Activos Fijos	01/02/2021	30/06/2021
	Publicación de Activos de Información	Validar y aceptar los activos de información para su publicación por cada líder de proceso	Área de sistemas Líder de Activos Fijos	01/07/2021	31/08/2021
		Publicar los instrumentos de activos de información consolidado	Área de sistemas Líder de Activos Fijos	01/07/2021	31/08/2021

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE DE LA TAREA	FECHA INICIO	FECHA FINAL
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el documento del Plan de Gestión de Cultura Organizacional	Líder de Talento Humano. Área de sistemas	01/02/2021	30/06/2021
		Publicar y Socializar el Plan de Gestión de Cultura Organizacional	Líder de Talento Humano. Área de sistemas Líder de Comunicaciones	01/02/2021	30/06/2021
	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Implementar las estrategias del Plan de Gestión de Cultura Organizacional	Líder de Talento Humano. Área de sistemas Líder de Comunicaciones	01/07/2021	31/10/2021
	Analizar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Analizar los instrumentos de medición del Plan de Gestión de Cultura Organizacional	Líder de Talento Humano. Área de sistemas	01/11/2021	31/12/2021
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Creación de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Área de sistemas	01/02/2021	30/06/2021
	Revisión de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Evidenciar el cumplimiento de los Requisitos Legales de Seguridad de la Información	Área de sistemas	01/02/2021	31/10/2021

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE DE LA TAREA	FECHA INICIO	FECHA FINAL
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Área de sistemas Acompaña: Oficina de planeación	01/02/2021	31/05/2021
	Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Área de sistemas Acompaña: Oficina de planeación	01/02/2021	31/05/2021
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Realimentación, revisión y verificación de los riesgos identificados	Área de sistemas Acompaña: Oficina de planeación	01/02/2021	30/06/2021
	Aceptación de Riesgos Identificados y publicación	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Área de sistemas Acompaña: Oficina de planeación	01/02/2021	31/08/2021
		Publicación Matriz de riesgos	Área de sistemas Acompaña: Oficina de planeación	01/02/2021	30/11/2021

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE DE LA TAREA	FECHA INICIO	FECHA FINAL
Gobierno Digital	Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	Área de sistemas	01/02/2021	30/06/2021
		Revisar y alinear la documentación del SGSI de la Entidad, de acuerdo con la Normatividad vigente.	Área de sistemas	01/02/2021	30/06/2021
		Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad	Área de sistemas	01/02/2021	31/07/2021
		Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información	Área de sistemas	01/02/2021	31/07/2021
Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo con los estándares emitidos por la Superintendencia de Industria y Comercios SIC	Área de sistemas	01/02/2021	31/12/2021
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos.	Área de sistemas	01/02/2021	31/12/2021
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Área de sistemas	01/02/2021	31/12/2021

DIEGO LEON MUÑOZ ZAPATA
Gerente E.S.E Hospital San Rafael de Itagüí.