PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CAMBIOS EFECTUADOS

No. VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
02	Diseño del plan institucional según lineamientos del Decreto 612 de 2018, orientado al cumplimiento de los objetivos y metas institucionales, priorizadas para la vigencia 2025	31-01-2025

	ELABORÓ	REVISÓ	APROBÓ
FECHA	**31-01-25**	**31-01-25**	**31-01-25**
CARGO	**Asesor Administrativo**	**Comité Institucional de Gestión y Desempeño**	**Gerente**

1. OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital.

1.1. OBJETIVOS ESPECÍFICOS

1. Establecer la estrategia de seguridad digital de la entidad.
2. Consolidar las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.
3. Priorizar los proyectos a implementar para la correcta implementación del SGSI.
4. Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

2. ALCANCE

El Plan Estratégico de Seguridad de la Información buscara la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la entidad, compartiendo el alcance definido dentro de la Política General de Seguridad de la Información, donde se indica que se tendrán en cuenta todos los procesos de la entidad. Por lo tanto en el desarrollo de este documento se requiere inicialmente hacer el diagnostico actual, para ello utilizamos el instrumento suministrado por el Ministerio de Tecnologías de la Información y las Comunicaciones, logrando obtener una visión general del estado en la cual se encuentra la Entidad y así lograr identificar sus debilidades y fortaleza.

Este Plan de Seguridad y Privacidad de la Información y su política, serán aplicables a todos los funcionarios de la entidad, a sus recursos, contratistas, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad y terceras partes, que usen activos de información que sean propiedad de la entidad.

3. DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- 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",

donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.

- Resolución No. 500 de 2021. "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.

4. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La entidad se ha venido organizando para promover el acceso, desarrollo, uso efectivo y apropiación social de las tecnologías de la información y las comunicaciones, la implementación de la política de seguridad de la información en la Entidad no depende únicamente del área de sistemas, es de todos, llevando una cultura organizacional que permita la protección y resguardo de la información. Este concepto es importante para la entidad y así dar su primer paso en la adopción de la Política de Seguridad y privacidad de la información firmada por la alta dirección y el Manual de la misma, en donde se informe el manejo de la información y lo importante que es para la entidad.

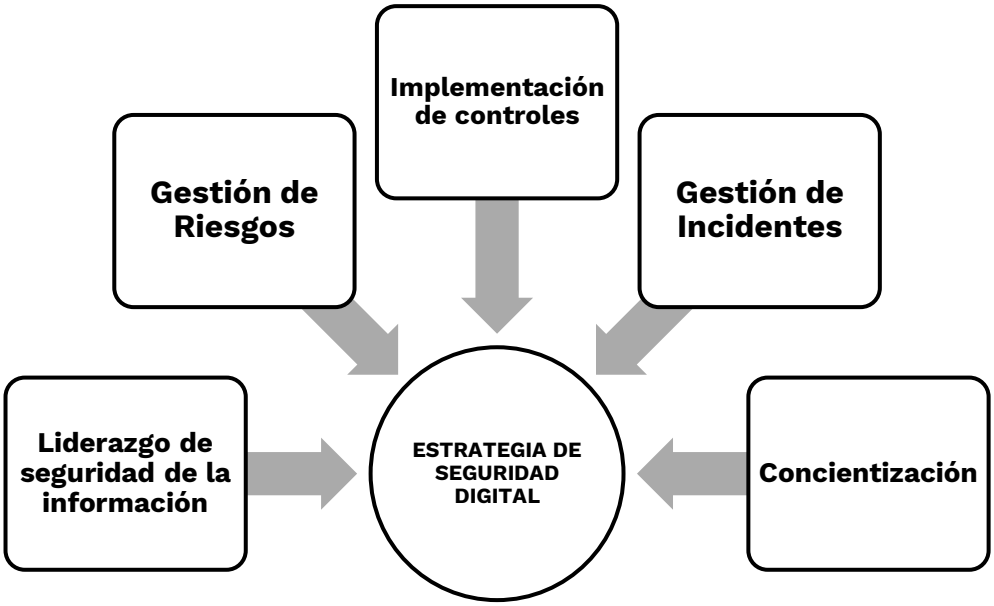
Se pueden encontrar algunas novedades con relación a seguridad de la información dentro de la entidad:

1. No se cuenta con una Política de Seguridad de la Información acorde a los nuevos lineamientos de la Resolución 500 de 2021 del MINTIC. "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".
2. Los sistemas de cableado y red de telecomunicaciones y eléctricos de la entidad presentan disposiciones inadecuadas y deficientes.
3. No existe un Plan Estratégico de Tecnología informática de largo plazo que comprenda las necesidades de equipos, programas y otros servicios.
4. No existe una política o plan estratégico para la compra y adquisición de equipos de cómputo los cuales cumplan los requisitos mínimos de seguridad.

5. ESTRATEGIA DE SEGURIDAD DIGITAL

La E.S.E Hospital San Vicente de Ramiriquí, establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información establecidos encuentran en la **Resolución No. 500 de 2021 y Anexo 1 del MINTIC** y de los cuales la entidad hará uso, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse, los cuales también hacen parte de la directrices de la resolución en mención.

Por tal motivo, se define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



5.1. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la Resolución No. 500 de 2021 del MINTIC:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la

	Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

5.2. PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, la Entidad, define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI) siguiendo lo establecido en la Resolución No. 500 de 2021 emitida por el MINTIC:

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	**PROYECTO 1:** Desarrollar e implementar una política de seguridad de conformidad a lo establecido en la Resolución No. 500 de 2021 del MINTIC.	Política de Seguridad Formalizada e Implementada.
	PROYECTO 2: Definición de Roles y Responsabilidades de Seguridad de la Información.	Definición de los Roles y Responsabilidades en Seguridad de la Información formalizados dentro de las políticas de seguridad.
	PROYECTO 3: Socialización de la Política de Seguridad implementada	Todo el personal de la entidad con el conocimiento de la política
	PROYECTO 4: Desarrollar e implementar un manual de políticas de seguridad de la información de conformidad a lo establecido en la Resolución No. 500 de 2021 del MINTIC.	Manual de políticas de seguridad de la información, focalizado e implementado
	PROYECTO 5: Socialización del Manual de políticas de Seguridad implementado	Todo el personal de la entidad con el conocimiento del manual
	PROYECTO 6: Realizar diagnóstico seguridad y privacidad	Documento de diagnóstico del estado actual en cuanto al estado de seguridad y privacidad de la información en la entidad
	PROYECTO 7: Actualización Diagnóstico de Seguridad y privacidad	Documento con el diagnostico de seguridad y privacidad actualizado
Gestión de riesgos	**PROYECTO 1:** Identificar, valorar y clasificar los riesgos asociados a los activos de información de conformidad a lo establecido en el	Matriz de riesgos de seguridad digital

	artículo 6 de la Resolución No. 500 de 2021 del MINTIC, donde están los lineamientos que se deben cumplir.	
	PROYECTO 2: Definir planes de tratamiento de riesgos de seguridad	Definir planes de tratamiento de riesgos
Concientización	**PROYECTO 1:** Establecer desde el inicio de cada año la planeación de sensibilización para todo el año.	Plan de Sensibilización
	PROYECTO 2: Realizar jornadas de sensibilización a todo el personal.	Evidencias de las actividades desarrolladas
	PROYECTO 3: Realizar trasferencia de conocimiento a colaboradores de la Entidad a través de cursos especializados en diferentes temas.	Certificaciones de cursos
Implementación de controles	**CONTROL 1** Política de respaldos de información.	Política de respaldos de información.
Gestión de incidentes	**PROYECTO 1:** Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información de conformidad a lo establecido en el artículo 9 de la Resolución No. 500 de 2021 del MINTIC, donde están los lineamientos que se deben cumplir.	Procedimiento de gestión de incidentes de seguridad formalizado.
	PROYECTO 2: Capacitar al personal en la gestión de incidentes de seguridad de la información.	Sesiones de capacitación desarrolladas.

5.3. CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

Para la elaboración del cronograma se debe contar con el recurso humano que tenga los conocimientos en seguridad de la información y con base a los proyectos definidos en la sección anterior, deberá establecer un cronograma de actividades donde se evidencie como se llevarán a cabo cada uno de los proyectos previstos. Las actividades podrán desarrollarse de forma secuencial o paralela según se considere.

ESTRATEGIA / EJE	PROYECTO	PERIODO EJECUCIÓN
Liderazgo de seguridad de la información	**PROYECTO 1:** Desarrollar e implementar una política de seguridad de conformidad a lo establecido en la Resolución No. 500 de 2021 del MINTIC.	Segundo trimestre 2025
	PROYECTO 2: Definición de Roles y Responsabilidades de Seguridad de la Información.	Segundo trimestre 2025

	PROYECTO 3: Socialización de la Política de Seguridad implementada	Segundo trimestre 2025
	PROYECTO 4: Desarrollar e implementar un manual de políticas de seguridad de la información de conformidad a lo establecido en la Resolución No. 500 de 2021 del MINTIC.	Tercer trimestre 2025
	PROYECTO 5: Socialización del Manual de políticas de Seguridad implementado	Tercer trimestre 2025
	PROYECTO 6: Realizar diagnóstico seguridad y privacidad	Mediano plazo
	PROYECTO 7: Actualización Diagnóstico de Seguridad y privacidad	Largo plazo
Gestión de riesgos	**PROYECTO 1:** Identificar, valorar y clasificar los riesgos asociados a los activos de información de conformidad a lo establecido en el artículo 6 de la Resolución No. 500 de 2021 del MINTIC, donde están los lineamientos que se deben cumplir.	Mediano plazo
	PROYECTO 2: Definir planes de tratamiento de riesgos de seguridad	Mediano plazo
Concientización	**PROYECTO 1:** Establecer desde el inicio de cada año la planeación de sensibilización para todo el año.	Mediano plazo
	PROYECTO 2: Realizar jornadas de sensibilización a todo el personal.	Mediano plazo
	PROYECTO 3: Realizar trasferencia de conocimiento a colaboradores de la Entidad a través de cursos especializados en diferentes temas.	Mediano plazo
Implementación de controles	**CONTROL 1:** Política de respaldos de información.	Mediano plazo
Gestión de incidentes	**PROYECTO 1:** Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información de conformidad a lo establecido en el artículo 9 de la Resolución No. 500 de 2021 del MINTIC, donde están los lineamientos que se deben cumplir.	Mediano plazo
	PROYECTO 2: Capacitar al personal en la gestión de incidentes de seguridad de la información.	Mediano plazo

Los proyectos que se encuentran para ejecución a **mediano plazo** serán modificados en una nueva versión de este documento cuando se cuente con el recurso humano idóneo para orientar dichas actividades.

Nota: Al finalizar cada vigencia, Se realizará una actualización del cronograma, incorporando el estado del avance de los proyectos formulados y si en efecto se cumplieron o se plantean aplazamientos para las vigencias posteriores. Así mismo, el cronograma podrá ser modificado o ajustado de acuerdo con las necesidades o situaciones que surjan en la entidad.

5.4. ANÁLISIS PRESUPUESTAL:

Con base a los proyectos definidos en el cronograma de actividades, se debe generar el presupuesto aproximado por cada vigencia según los proyectos establecidos y presentarlo a la Alta Dirección para las consideraciones y viabilidad pertinentes:

ESTRATEGIA / EJE	PROYECTO	VIGENCIA EJECUCIÓN	INVERSIÓN
Liderazgo de seguridad de la información	**PROYECTO 1:** Desarrollar e implementar una política de seguridad de conformidad a lo establecido en la Resolución No. 500 de 2021 del MINTIC.	2024 - 2025	$0
	PROYECTO 2: Definición de Roles y Responsabilidades de Seguridad de la Información.	2024 - 2025	$0
	PROYECTO 3: Socialización de la Política de Seguridad implementada	2024 - 2025	$0
	PROYECTO 4: Desarrollar e implementar un manual de políticas de seguridad de la información de conformidad a lo establecido en la Resolución No. 500 de 2021 del MINTIC.	2024 - 2025	$0
	PROYECTO 5: Socialización del Manual de políticas de Seguridad implementado	2024 - 2025	$0
	PROYECTO 6: Realizar diagnóstico seguridad y privacidad	Mediano plazo	Por Definir
	PROYECTO 7: Actualización Diagnóstico de Seguridad y privacidad	Largo plazo	Por Definir
Gestión de riesgos	**PROYECTO 1:** Identificar, valorar y clasificar los riesgos asociados a los activos de información de conformidad a lo establecido en el artículo 6 de la Resolución No. 500 de 2021 del MINTIC, donde están los lineamientos que se deben cumplir.	Mediano plazo	Por Definir
	PROYECTO 2: Definir planes de tratamiento de riesgos de seguridad	Mediano plazo	Por Definir
Concientización	**PROYECTO 1:** Establecer desde el inicio de cada año la planeación de sensibilización para todo el año.	Mediano plazo	Por Definir
	PROYECTO 2: Realizar jornadas de sensibilización a todo el personal.	Mediano plazo	Por Definir
	PROYECTO 3: Realizar trasferencia de conocimiento a colaboradores de la Entidad a través de cursos especializados en diferentes temas.	Mediano plazo	Por Definir
	PROYECTO 4: Medir el grado de sensibilización a toda la Entidad.	Mediano plazo	Por Definir
Implementación de controles	**CONTROL 1:** Política de respaldos de información.	Mediano plazo	Por Definir
	CONTROL 2: Procedimiento de Gestión de Cambios.	Mediano plazo	Por Definir
	CONTROL 3: Clasificación de la información.	Mediano plazo	Por Definir

	CONTROL 4: Políticas de Desarrollo Seguro	Mediano plazo	Por Definir
	CONTROL 5: Implementación de solución WAF	Mediano plazo	Por Definir
Gestión de incidentes	**PROYECTO 1:** Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información de conformidad a lo establecido en el artículo 9 de la Resolución No. 500 de 2021 del MINTIC, donde están los lineamientos que se deben cumplir.	Mediano plazo	Por Definir
	PROYECTO 2: Capacitar al personal en la gestión de incidentes de seguridad de la información.	Mediano plazo	Por Definir

Los proyectos que se encuentran sin definir presupuesto de inversión, serán modificados en una nueva versión de este documento cuando se cuente con el recurso humano idóneo para orientar dichas inversiones o presupuestos.

6. RESPONSABLES

1. Gerente: Aprobar los documentos de Alto Nivel

7. APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección, el comité de gestión y desempeño institucional, con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.