PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

ELABORADO POR:

GERXON MAURICIO ESPINOSA SATIVA

SANATORIO DE AGUA DE DIOS E.S.E.

MACROPROCESO GESTION DE APOYO

PROCESO GESTION TECNOLOGICA

2024 - 2026

FECHA DE APROBACIÓN: 16/12/2024

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En Colombia, la implementación del Gobierno en línea ha sido sistemática y coordinada en todas las instituciones públicas. En años recientes, se han observado modificaciones y progresos en la utilización y adopción de la tecnología como instrumento que facilita la mejora de la administración pública, la prestación de servicios y la transparencia.

En el desempeño de sus tareas, el Sanatorio de Agua de Dios E.S.E elabora, implementa y lleva a cabo estrategias para evitar, manejar y disminuir los riesgos asociados a la seguridad y privacidad de la información, los cuales pueden impactar la continuidad de los servicios de la institución.

En la administración de los procesos estratégicos, misionales y de soporte, se están procesando, administrando, guardando, protegiendo, transfiriendo e intercambiando datos importantes que no deben ser revelados a personal no autorizado, ya que podrían comprometer legalmente al Sanatorio de Agua de Dios E.S.E.

En última instancia, las directrices y proyectos destinados al desarrollo, mejora e implementación eficaz de los Sistemas de Información, junto con las iniciativas que facilitarán una correcta administración de la Infraestructura de Hardware/Software, fundamentados en el Modelo de Seguridad y Privacidad de la Información (MSPI) y en las óptimas prácticas de Gestión de Servicios y Proyectos de Tecnología de la Información, no solo apoyarán la consecución de los objetivos institucionales.

2. OBJETIVO

Fortalecer la integridad, privacidad y disponibilidad de los recursos informativos en Sanatorio de Agua de Dios, con el fin de disminuir los peligros a los que se enfrenta la organización hasta niveles tolerables, mediante la puesta en marcha de las estrategias de seguridad digital establecidas en este documento para los periodos 2024-2026.

2.1 OBJETIVOS ESPECÍFICOS

- Establecer y determinar la estrategia de seguridad digital de la entidad.
- Aumentar el grado de madurez en la administración de la seguridad de la información
- Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MPSI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Organizar el análisis y monitoreo de los controles y directrices establecidos dentro del contexto del Sistema de Gestión de Seguridad de la Información.

3. ALCANCE

El Plan Estratégico de Seguridad de la Información, que persigue la puesta en marcha del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la organización, sigue el ámbito establecido en la Política General de Seguridad de la Información, donde se señala que se considerarán todos los procedimientos de la institución.

4. DEFINICIONES

- Activos- Respecto a la seguridad de la información, hace referencia a cualquier datos o componente vinculado con su manejo (computadores, aplicativos, soportes, edificios, personas y entre otros) que represente un valor para la organización. (ISO/IEC 27000).
- Riesgo - Es posible que una amenaza específica pueda aprovechar una debilidad para provocar una pérdida o perjuicio en un recurso de información. Normalmente se percibe como una mezcla de la probabilidad de un suceso y sus repercusiones. (ISO/IEC 27000).
- Sistema de Gestión de Seguridad de la Información SGSI - Conjunto de componentes interconectados o enlazados (estructura organizativa, políticas, organización de actividades, responsabilidades, procesos, procedimientos y recursos) que emplea una entidad para definir una política y metas de seguridad de la información y lograr estas metas, apoyándose en un enfoque de administración y mejora constante. (ISO/IEC 27000).
- Procedimiento - Los procedimientos representan la explicación minuciosa de cómo se implementa una política.
- Integridad - Conservación de la precisión y totalidad de la información y sus procedimientos.
- Confidencialidad - La información no se ofrece ni se divulga a personas, entidades o procedimientos no autorizados.
- Disponibilidad - Acceso y uso de la información y los sistemas para su tratamiento por parte de las personas, organismos o procedimientos autorizados cuando sea necesario.
- Control - Las políticas, procedimientos, prácticas y estructuras organizativas ideadas para reducir los riesgos de seguridad de la información a un nivel inferior al nivel de riesgo aceptado. También se emplea el término control como sinónimo de protección o contramedida. En una versión más sencilla, se refiere a una medida que altera el riesgo.
- Política - Es la guía o directrices que todos los integrantes de la entidad deben divulgar, comprender y seguir.
- Análisis de Riesgo - Procedimiento para entender la esencia del riesgo y establecer el grado de riesgo. (ISO/IEC 27000).

5. MARCO NORMATIVO

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 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".
- ISO/IEC 27001 - Seguridad de la Información.
- ISO 31000 – Gestión de Riesgos.
- Ley 1581 de 2012 - "Protección de Datos personales".
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.

6. DESARROLLO DEL CONTENIDO

La protección y confidencialidad de los datos es un elemento esencial de la Estrategia de Gobierno digital. Este se corresponde con la puesta en marcha del modelo de seguridad orientado a mantener la privacidad, la integridad y la disponibilidad de la información, lo que favorece la realización de la misión y metas estratégicas del Sanatorio de Agua de Dios E.S.E.

El Sanatorio de Agua de Dios E.S.E ha avanzado en la implantación de este modelo de seguridad y el objetivo es seguir madurándolo en la vigencia 2024-2026, cumpliendo con el ciclo del modelo de seguridad y privacidad de la información, donde se enfatiza en una mejora continua. Este modelo se está implantando apoyado también en el estándar de seguridad ISO 27001:2013.

6.1 DIAGNÓSTICO DEL ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para establecer el estado actual, el Sanatorio de Agua de Dios E.S.E ha ejecutado el diagnóstico basado en el instrumento de medición propuesto MSPI por el MinTIC, los cuales se presentan a continuación:

6.1.1 ESTADO DEL SGSI BASADO EN EL INSTRUMENTO DE MEDICIÓN DEL MSPI

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	78	100	**GESTIONADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	72	100	**GESTIONADO**
A.8	GESTIÓN DE ACTIVOS	59	100	**EFECTIVO**
A.9	CONTROL DE ACCESO	87	100	**OPTIMIZADO**
A.10	CRIPTOGRAFÍA	80	100	**GESTIONADO**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	82	100	**OPTIMIZADO**
A.12	SEGURIDAD DE LAS OPERACIONES	89	100	**OPTIMIZADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	98	100	**OPTIMIZADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	99	100	**OPTIMIZADO**
A.15	RELACIONES CON LOS PROVEEDORES	80	100	**GESTIONADO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	91	100	**OPTIMIZADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	64	100	**GESTIONADO**
A.18	CUMPLIMIENTO	52,5	100	**EFECTIVO**
PROMEDIO EVALUACIÓN DE CONTROLES		**80**	**100**	**OPTIMIZADO**

El Sanatorio de Agua de Dios E.S.E ha colaborado en la evolución del SGSI implementando métodos, instrucciones, concienciaciones sobre seguridad, entre otros. Los controles que han sido trabajados y desarrollados son de estos asuntos, tal como se puede apreciar una evaluación eficaz de controles A ISO27001:2013.

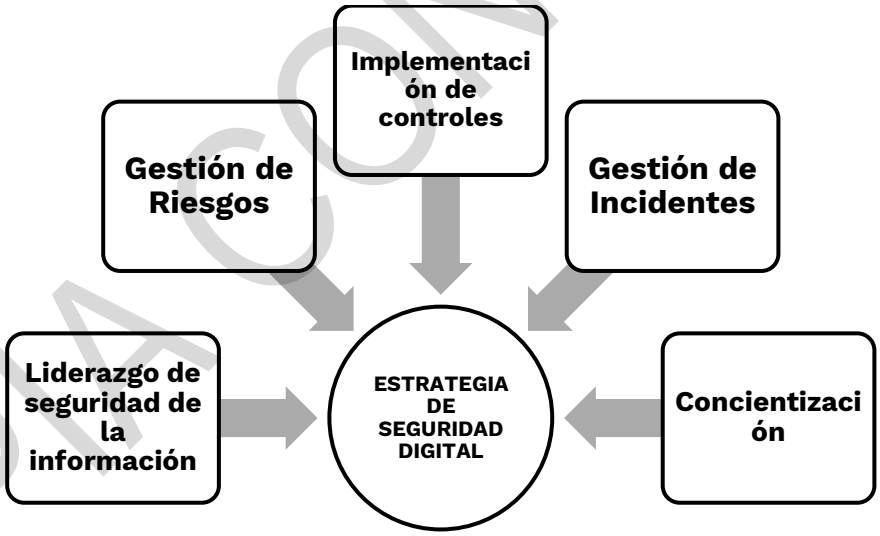
- Políticas de seguridad de la información
- Activos de información
- Control de accesos
- Criptografía

- Seguridad física y del entorno
- Desarrollo de software
- Seguridad en redes
- Backups
- Seguridad de los recursos humanos
- Gestión de la continuidad del negocio
- Gestión de riesgos de seguridad de la información

Sin embargo, aún falta trabajar varios controles en el plan presentado en este documento, sin dejar de trabajar en mantener los que ya están en estado administrado y optimizado.

6.2 ESTRATEGIA DE SEGURIDAD DIGITAL

El Sanatorio de Agua de Dios E.S.E define una estrategia de seguridad digital que incorpora los principios, políticas, procedimientos, guías, manuales, formatos y directrices para la administración de la seguridad de la información. La base de esta estrategia radica en la aplicación del Modelo de Seguridad y Privacidad de la Información -MSPI, además de la guía para la administración de riesgos de seguridad de la información y el procedimiento de administración. Además, labora en su SGSI conforme a la norma de seguridad ISO27001:2013.



6.3 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, según MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Garantizar la instauración del Modelo de Seguridad y Privacidad de la Información (MSPI) mediante la aprobación de la política general y otras directrices establecidas con el objetivo de salvaguardar la privacidad, integridad y disponibilidad de la información. El pilar esencial es el compromiso de la alta dirección y los líderes de las distintas áreas y/o procesos de la organización, mediante la definición de los roles y obligaciones en seguridad de la información.
Gestión de riesgos	Establecer los riesgos de seguridad de la información a través de la planificación y evaluación establecida con el objetivo de evitar o disminuir los impactos no deseados, ya que simulan la puesta en marcha de controles de seguridad para su tratamiento.
Concientización	Potenciar la formación de la cultura organizacional fundamentada en la seguridad de la información para que se transforme en un hábito, fomentando las políticas, procedimientos, normas, buenas prácticas y otras directrices, la transmisión de saberes, la distribución y comunicación de obligaciones de todos los empleados de la entidad en relación a la seguridad y privacidad de la información.
Implementación de controles	Organizar e instaurar las medidas requeridas para alcanzar las metas de seguridad y privacidad de la información, y preservar la confianza en la realización de los procedimientos de la organización, pueden ser su dirigidas en controles tecnológicos y/o administrativos.
Gestión de incidentes	Asegurar una gestión de incidentes de seguridad informática basada en un enfoque de integración, análisis y comunicación de los sucesos e incidentes y las vulnerabilidades de seguridad, con el objetivo de identificarlos y solucionarlos para reducir el efecto adverso de estos en la organización.

6.4 PORTAFOLIO DE PROYECTOS / ACTIVIDADES

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	Capacitar la política de seguridad Definición de Roles y Responsabilidades de Seguridad de la Información.	Asistencia de las capacitaciones Definición de los Roles y Responsabilidades en Seguridad de la Información formalizados dentro de las políticas de seguridad.
Gestión de riesgos	Gestión de riesgos y planes de tratamiento de riesgos de seguridad de la información	4 informes de seguimiento a de riesgos de seguridad de la información
Concientización	Desarrollo de actividades de uso y apropiación del Modelo de Seguridad y Privacidad de la Información	Evidencias de las capacitaciones y socialización realizadas.
Implementación de controles	Procedimiento de respaldos de información. Procedimiento aseguramiento de servicios en la red Clasificación de activo de información. Políticas de seguridad física Procedimiento de revisión de firewall y servidor proxy Procedimiento de gestión de usuarios y contraseñas Gestionar la compra de licencia de antivirus	Procedimiento de respaldos de información. Procedimiento aseguramiento de servicios en la red Clasificación de activo de información. Políticas de seguridad física Procedimiento de revisión de firewall y servidor proxy Procedimiento de gestión de usuarios y contraseñas Gestionar la compra de licencia de antivirus

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Gestión de incidentes	Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información. Procedimiento de capacitación y sensibilización del personal	Procedimiento de gestión de incidentes de seguridad formalizado. Procedimiento de capacitación y sensibilización del personal

6.5 CRONOGRAMA PROYECTOS / ACTIVIDADES

Año 2025				Año 2026			
Trimestre1	**Trimestre2**	**Trimestre 3**	**Trimestre 4**	**Trimestre1**	**Trimestre2**	**Trimestre3**	**Trimestre4**
Realizar diagnóstico seguridad y privacidad		Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información.	Capacitar al personal en la gestión de incidentes de seguridad de la información.	Actualización Diagnóstico de Seguridad	Capacitar al personal en la gestión de incidentes de seguridad de la información.	Capacitar al personal en la gestión de incidentes de seguridad de la información.	
Realizar primer informe de seguimiento a de riesgos de seguridad de la información	Realizar s informe de seguimiento a de riesgos de seguridad de la información	Realizar tercer informe de seguimiento a de riesgos de seguridad de la información	Realizar cuarto informe de seguimiento a de riesgos de seguridad de la información	Realizar primer informe de seguimiento a de riesgos de seguridad de la información	Realizar s informe de seguimiento a de riesgos de seguridad de la información	Realizar tercer informe de seguimiento a de riesgos de seguridad de la información	Realizar cuarto informe de seguimiento a de riesgos de seguridad de la información

Definición de Roles y Responsabilidades de Seguridad de la Información.		Capacitar política en seguridad de la información y roles de seguridad de la información de la empresa.		Capacitar política en seguridad de la información y roles de seguridad de la información de la empresa.	Capacitar política en seguridad de la información y roles de seguridad de la información de la empresa.
Desarrollo de actividades de uso y apropiación del Modelo de Seguridad y Privacidad de la Información		Capacitar y socializar del uso y apropiación del Modelo de Seguridad y Privacidad de la Información		Capacitar y socializar del uso y apropiación del Modelo de Seguridad y Privacidad de la Información	Capacitar y socializar del uso y apropiación del Modelo de Seguridad y Privacidad de la Información
		Procedimiento de respaldos de información. Procedimiento aseguramiento de servicios en la red Clasificación de activo de información. Políticas de seguridad física Procedimiento de revisión de firewall y servidor proxy Procedimiento de gestión de usuarios y contraseñas Gestionar la compra de licencia de antivirus		Capacitar todos los procedimientos de control	Capacitar todos los procedimientos de control Gestionar la compra de licencia de antivirus
		Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información.	Capacitar el procedimiento de gestión de incidentes	Capacitar el procedimiento de gestión de incidentes	Capacitar el procedimiento de gestión de incidentes

6.6 ANÁLISIS PRESUPUESTAL

Año 2025		Año 2026	
Proyecto	**Inversión**	**Proyecto**	**Inversión**
Contratista de apoyo para mantener el modelo de seguridad de la información	$ 57.600.000	Contratista de apoyo para mantener el modelo de seguridad de la información	$ 60.000.000
Gestionar la compra de licencia de antivirus	$12.000.000	Gestionar la compra de licencia de antivirus	$13.000.000

6.7 RESPONSABLES

- Responsable de la Oficina de Tecnología y Sistemas de la información (TIC) ´ Sistemas
- Coordinador GIT Planeación, Gestión documental y TIC´S.

7. ANEXOS

NO APLICA.

8. FORMATOS

NO APLICA.

9. DOCUMENTOS RELACIONADOS

- Instrumento de evaluación del Modelo seguridad y Privacidad de la información (MSPI)

10. REFERENCIAS

- Gobierno digital. (s. f.). https://gobiernodigital.mintic.gov.co/692/articles-176929_recurso_1.docx

11. APROBACIÓN

ELABORÓ	REVISÓ	APROBÓ	Vo.Bo. SGC
Gerxon Mauricio Espinosa Sativa Profesional de Apoyo Oficina TIC`S	Edgar Angelico Gamboa Mur Responsable de TIC´S Cesar Mauricio Ubaque Téllez GIT de Planeación, Gestión Documental y TIC`S	Antonio Ruiz Flórez Gerente	Cesar Mauricio Ubaque Téllez GIT de Planeación, Gestión Documental y TIC`S
FECHA	FECHA	FECHA	FECHA
16/12/2024	16/12/2024	16/12/2024	16/12/2024

12. CONTROL DE CAMBIOS

TIPO DE MODIFICACIÓN	DESCRIPCIÓN DEL CAMBIO	RESPONSABLE	FECHA DEL CAMBIO	VERSIÓN
CREACIÓN	Creación del documento	Gerxon Mauricio Espinosa Sativa Profesional de Apoyo Oficina TIC`S	16/12/2024	UNO