Plan Estratégico de Seguridad de la Información del Sector 2025-2028

Contrato 1588 de 2024

Bogotá, diciembre de 2024

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

CONTROL DE CAMBIOS			
VERSIÓN	**FECHA**	**NATURALEZA DE LA VERSIÓN**	**APROBADO POR**
1.0	29/12/2024	Versión inicial	N/A

ALCANCE CONTRACTUAL			
FASE	**ETAPA**	**OBLIGACIÓN CONTRACTUAL**	**ENTREGABLE**
Construir	PESI construido	Construir el Plan Estratégico de Seguridad de la Información Institucional y Sectorial con los insumos obtenidos.	Documento con el Plan Estratégico de Seguridad de la información del sector.

1. INTRODUCCIÓN

La protección de la información es una prioridad fundamental para las organizaciones en general y el sector salud en Colombia en particular. La digitalización y la interoperabilidad de los servicios de salud han transformado la eficiencia y la calidad de la atención médica, permitiendo un acceso confiable a la información de los pacientes y facilitando la gestión de los servicios sanitarios en nuestro país.

Las entidades adscritas al Ministerio de Salud y Protección Social (MSPS) deben aplicar medidas consistentes y alineadas con los lineamientos aprobados por el Ministerio. Estas entidades deben colaborar en estrategias transversales que fortalezcan la protección de la información, garanticen la interoperabilidad de los servicios y promuevan la confianza digital en el sector, contribuyendo a la eficacia y eficiencia en la prestación de servicios de salud para la ciudadanía y la comunidad en general.

La transformación digital apoya el desarrollo del sector Salud y de las entidades adscritas, aunque de manera concomitante podría incrementarse la superficie de exposición de riesgos que afecten los principios de integridad, confidencialidad y disponibilidad de la información. Para poder mantener de manera paralela el desarrollo del sector salud y los riesgos en un nivel aceptable se requiere contar una estrategia de seguridad de la información. Lo anteriormente expresado está apoyado en la Transformación Digital Pública, artículo 148; Gobierno Digital como política de gestión y desempeño institucional y su Decreto 767 de 2022, entre otras normas

El presente documento se construye en el marco del desarrollo de la elaboración y socialización de los planes de transformación digital para las entidades adscritas al MSPS, dentro de los cuales se incluye el Plan Estratégico de Seguridad Información (PESI) y constituye el documento principal donde se formula la estrategia de protección de la información, seguridad digital y protección de datos personales, de conformidad con los lineamientos metodológicos del Ministerio de Tecnologías de las comunicaciones (MinTIC) para su construcción.

El Plan Estratégico de Seguridad de la Información es un instrumento esencial para fortalecer la protección de la información en el ecosistema de salud colombiano. Este plan se alinea con las mejores prácticas internacionales y las normativas locales vigentes, garantizando que el sector salud opere de manera que mejore la calidad de vida de los ciudadanos. La elaboración del PESI se basa en la plantilla desarrollada por el MinTIC para cumplir con los requisitos

establecidos en el artículo 5 de la Resolución 500 de 2021, relacionada con la estrategia de seguridad digital.

Finalmente, este documento presenta las actividades realizadas para crear el PESI Sectorial. El primer hito corresponde al diagnóstico del estado actual de la seguridad de la información en las entidades adscritas, identificando brechas y oportunidades de mejora que sirven como insumos para la planeación del PESI Sectorial. El segundo hito aborda la estructuración de iniciativas y proyectos diseñados para reducir los riesgos identificados en el primer hito. Además, este documento detalla las fases propuestas para la construcción del PESI Sectorial: comprender, analizar, construir y presentar. Esta metodología fue aplicada a cada entidad para elaborar el PESI del sector, que, junto con el PESI Institucional, busca mejorar la protección de la información en el sector salud.

2. OBJETIVOS

2.1. Objetivo General

Fortalecer la seguridad de la información en el Ministerio de Salud y Protección Social – MSPS mediante la definición y establecimiento de la estrategia de seguridad digital del sector para el período 2024-2028, alineada con los necesidades del sector y las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), la Resolución 500 de 2021, el Plan Nacional de Desarrollo y mejores prácticas en seguridad vigentes y aplicables, fomentando una cultura de seguridad y privacidad que asegure la confidencialidad, integridad y disponibilidad de los activos de información del sector.

2.2. Objetivos Específicos

A continuación, se exponen los objetivos específicos del PESI Sectorial:

- Definir la estrategia de seguridad digital para el sector
- Establecer las necesidades del sector para el fortalecimiento del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos a implementar para el fortalecimiento del SGSI del sector.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información del sector

3. ALCANCE

El alcance de este documento está orientado en definir conceptualmente el diagnóstico de situación actual y las iniciativas del PESI. Por otra parte, aplica a todos los procesos y activos de información de las entidades adscritas al MSPS. Los proyectos aquí presentados deben ser integrados en la infraestructura existente y gestionados de acuerdo con las mejores prácticas con el fin de apoyar en la consecución de los objetivos estratégicos del sector salud.

4. MARCOS METODOLÓGICOS

4.1. Marco Metodológico General del Proyecto

Con el propósito de presentar los marcos metodológicos utilizados para la elaboración del PESI Sectorial, a continuación, se presenta una breve descripción de las fases para la construcción del PESI desde la perspectiva general del proyecto. Para el sector se tuvo en cuenta comprender la situación actual en lo referente a la protección de la información, luego se procedió al análisis de la información recolectada a manera de insumos, con base en lo anterior se construyen los diferentes artefactos para definir el catálogo de iniciativas y la hoja de ruta y finalmente se realiza la transferencia de conocimiento a las entidades sectoriales y sus respectivos representantes.

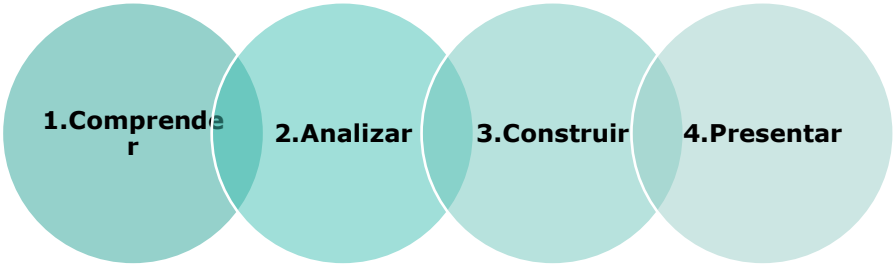

Ilustración 1 Fases del proyecto PESI

Fuente: MSPS.

Fase Comprender: en esta fase se realizaron entrevistas y recopilación de documentos a nivel Sectorial con el fin de entender la situación actual en seguridad de la información de tal manera que el PESI Sectorial considere proyectos de la mayor relevancia para ser implementados según la hoja de ruta aquí también definida.

Fase Analizar: en esta fase se realiza el estudio de la situación actual de las entidades adscritas con base en la etapa anterior con el fin de identificar el nivel de madurez que se tiene al momento de este ejercicio garantizando así que los proyectos establecidos ayuden a mitigar las brechas encontradas.

Fase Construir: en esta fase de la construcción del PESI Sectorial se definirán los proyectos que se deben ejecutar, planteando iniciativas o proyectos que conformen un portafolio que oriente las inversiones en seguridad digital en los siguientes cuatro años, partiendo de los hallazgos o debilidades encontradas, el cierre de las brechas tecnológicas identificadas y las oportunidades relacionadas con nuevas tendencias tecnológicas en seguridad de la información.

Presentar: en esta fase se realiza la socialización y la transferencia de conocimiento con el fin de que las entidades adscritas al MSPS cuenten con los conocimientos mínimos necesario para que desde todas las áreas tengan la conciencia de la importancia de la mejora continua en seguridad digital a lo largo de todo el Sector.

4.2. Política de Gobierno Digital

La Estrategia de Gobierno en Línea en Colombia, la evolución constante de la sociedad, y el avance del país hacia una economía digital requieren el desarrollo de procesos de transformación digital al interior del Estado, para lograr mejores condiciones de vida para los ciudadanos, así como satisfacer necesidades y problemáticas a través del aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC). En la siguiente figura se muestra el proceso completo que involucra la Política de Gobierno Digital (PGD) incluyendo las siguientes etapas: Conocer, Planear, Ejecutar y Medir.

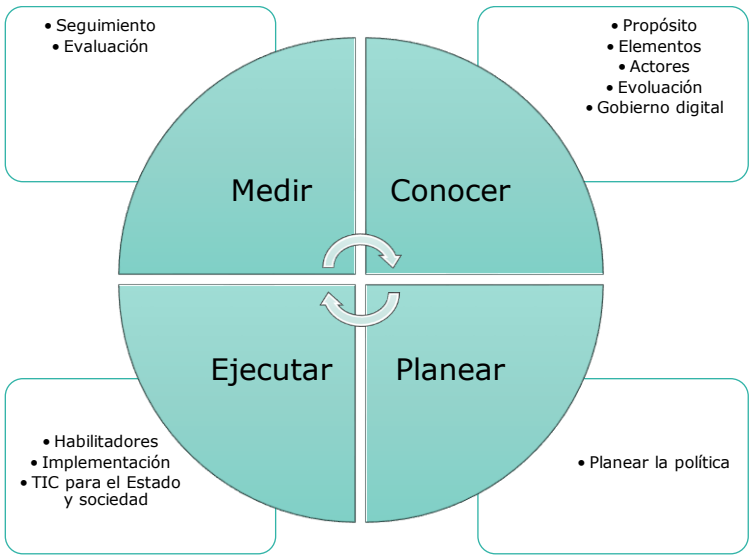

Ilustración 2 Fases de la Política de Gobierno Digital

Fuente: MinTIC, MAE Dominio de Arquitectura de Seguridad.

Finalmente, la PGD permite y estimula el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Las entidades adscritas al MSPS deben cooperar activamente en el cumplimiento de las mejores prácticas en seguridad de la información y las nuevas tendencias que en esta disciplina se presenten con el fin de estructurar sus políticas con los lineamientos recibidos por parte del ente rector para implementar una serie de medidas de proyección alineadas con los objetivos estratégicos del Sector.

4.3. Modelo MAE de Arquitectura Empresarial

Conforme al Modelo de Arquitectura Empresarial (MAE) del MinTIC, dominio de Seguridad de la información, está alineado con en el marco de referencia; Arquitectura de Seguridad Empresarial Aplicada de Sherwood (SABSA), que establece los servicios de seguridad necesarios para proteger la información institucional. Este enfoque permite alinear la seguridad con los objetivos estratégicos de la Entidad y mitigar los riesgos que se hayan identificados.

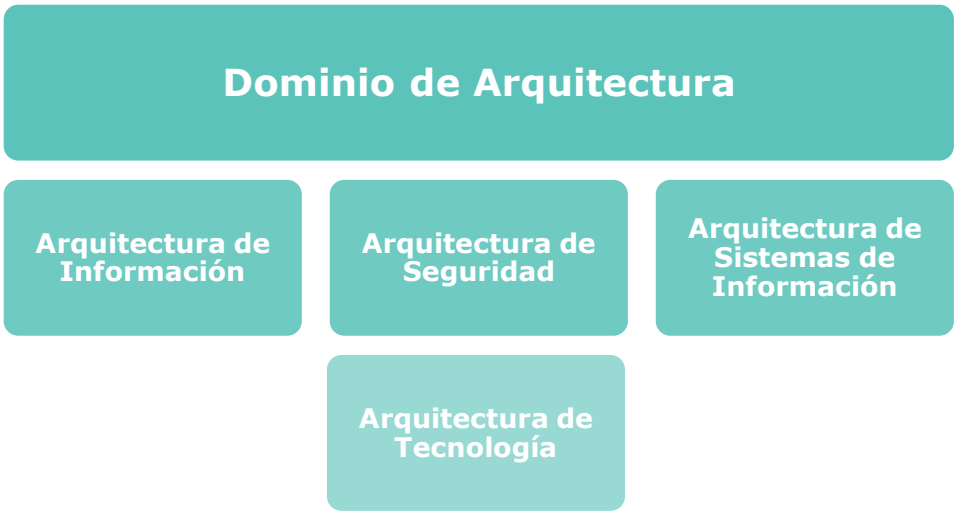

Ilustración 3 Modelo MAE de arquitectura empresarial.

Fuente: MinTIC, MAE.

Una arquitectura de seguridad no debe existir aislada de otros componentes al interior de la entidad. La seguridad de la información debe integrarse de modo estratégico. Se basa en la información de las entidades, que ya está disponible en los ejercicios que se hayan realizado de arquitectura empresarial y esta arquitectura de seguridad genera artefactos e información que deberían ser integrado por los artefactos hasta ahora realizados de arquitectura empresarial. Ésta es la razón por la cual se recomienda que exista una estrecha integración y colaboración de la arquitectura de seguridad y la arquitectura empresarial. Es decir que la arquitectura de seguridad está integrada con la arquitectura institucional, la de información, la de sistemas de información y con el dominio de arquitectura de tecnología.

Finalmente, SABSA es un marco de referencia y una metodología integral diseñada para desarrollar arquitecturas de seguridad de la información basadas en riesgos. Su enfoque se centra en alinear la seguridad de la información con los objetivos estratégicos del negocio, ofreciendo así un proceso estructurado y

sistemático para la gestión de los riesgos de seguridad. MAE es un marco más amplio para la gestión de toda la arquitectura empresarial, incluyendo la tecnológica, los procesos, los datos y de aplicaciones, además incluye un dominio la Arquitectura de Seguridad.

4.4. Modelo de Seguridad y Privacidad de la Información

El MinTIC ha elaborado el MSPI para la implementación de la estrategia de seguridad digital y un sistema de gestión de seguridad de la información (SGSI), teniendo como referencia el ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; por otro lado, el modelo consta de cinco (5) fases tal como se presenta a continuación:

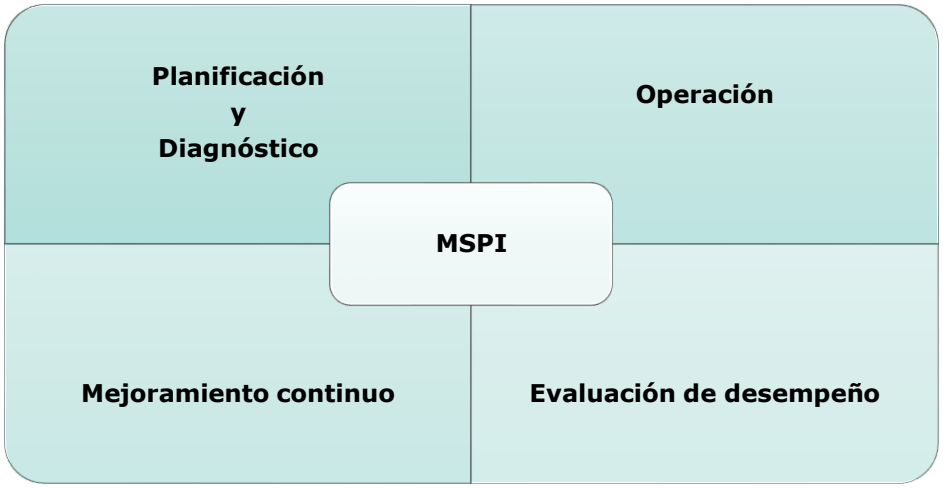

Ilustración 4 Modelo de Seguridad y Privacidad de la Información

Fuente: MSPI, MinTIC.

Diagnóstico: en la fase inicial se requiere realizar un diagnóstico con respecto a la protección de la información.

Planificación: determinar las necesidades y objetivos de seguridad y privacidad de la información.

Operación: se implementan los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos.

Evaluación de desempeño: se determina la forma de evaluación para la adopción del modelo de seguridad.

Mejoramiento Continuo: se establecen los procedimientos para optimizar el modelo.

4.5. Modelo Gartner de Nivel de Madurez

La forma en que se toman decisiones erróneas en materia de gestión de datos varía de una organización a otra, pero casi siempre se debe a la misma razón: prácticas de gobernanza de datos deficientes. Para mejorar la gobernanza de datos se necesitan dos cosas: saber dónde se encuentra la empresa en este momento y qué es exactamente lo que debe cambiar.

Gartner lleva décadas asesorando a organizaciones de todo tipo sobre sus políticas de gobernanza de datos, evaluando qué funciona y qué no. Convirtieron esta experiencia en un modelo de madurez de la gestión de la información que cualquier empresa puede utilizar para evaluar y mejorar sus propias prácticas.

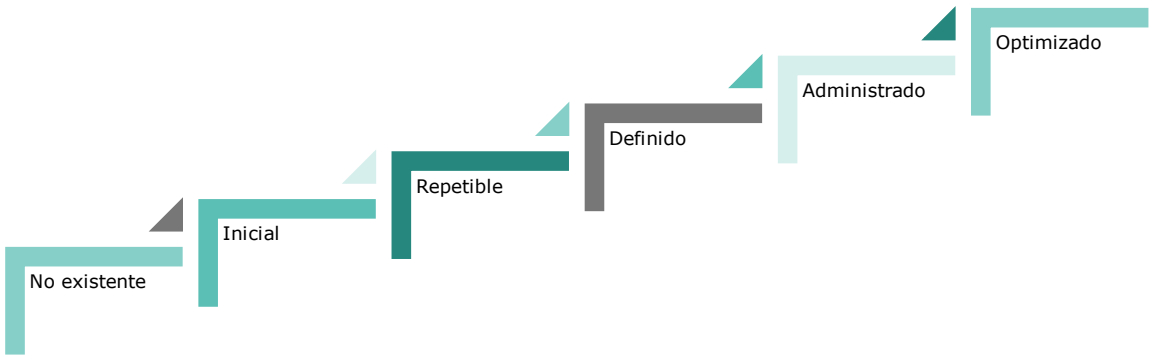

Ilustración 5 Niveles de madurez según Gartner.

Fuente: MinTIC, MSPI, Gartner.

Los niveles de madurez que se usarán en este documento siguiendo los lineamientos estipulados por la firma Gartner son:

No Existente: la entidad no cuenta con ningún artefacto relacionado con el lineamiento.

Inicial: la entidad cuenta con algunos artefactos relacionados con el lineamiento, pero sin actualizar, ni estandarizar.

Repetible: la entidad cuenta con todos los artefactos estandarizados de acuerdo con el lineamiento, pero no todos están actualizados. Estos son actualizados a

discreción en los diferentes proyectos e iniciativas sin existir un lineamiento que soporte su aplicación.

Definido: la entidad cuenta con todos los artefactos estandarizados y actualizados (con fecha máxima de hace 1 año). Adicional a esto, se encuentran formalizados a través de lineamientos y son conocidos por las partes interesadas.

Administrado: la entidad cuenta con todos los artefactos estandarizados (con fecha máxima de un año) en el repositorio respectivo y son actualizados de acuerdo con los lineamientos establecidos.

Optimizado: la entidad cuenta con todos los artefactos estandarizados y actualizados (con fecha máxima de un año) y se realiza una mejora continua de los artefactos de acuerdo con las mejores prácticas de cada dominio.

4.6. Metodología del MINTIC para el PESI

La Plantilla establecida por el MINTIC busca fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de las entidades a nivel nacional, 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 previamente definidas. Se busca cumplir con los requisitos del establecimiento de la estrategia de seguridad digital, de acuerdo con lo establecido en el artículo cinco (5) de la resolución 500 de 2021. A continuación, se presenta los pilares para la construcción del documento PESI.

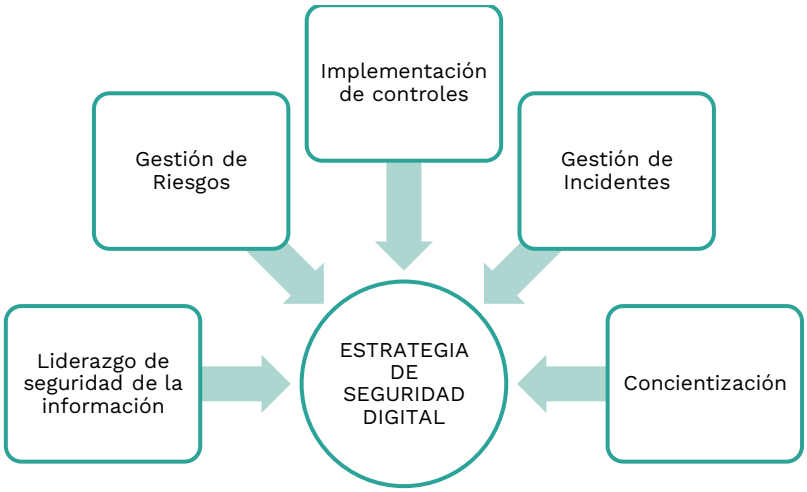

Ilustración 6 Metodología o plantilla para el PESI.

Fuente: MinTIC.

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 500 de 2021:

Liderazgo de seguridad de la información: asegurar que se establezca el MSPI a través de la aprobación de la política general y demás lineamientos que se definan.

Gestión de riesgos: determinar los riesgos de seguridad de la información a través de la planificación y valoración 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 del diario proceder.

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 las entidades sectoriales.

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 en seguridad de la información. Las entidades adscritas deben cooperar con el MSPS con el fin de establecer una gestión de incidentes transversal.

4.7. Marco Metodológico DOFA y PESTEL

En la construcción del PESI del Sector, se requiere analizar las debilidades, fortalezas, oportunidad y amenazas del área de seguridad de la información de la OTIC con el fin de elaborar estrategias que maximicen las fortalezas y disminuyan las amenazas, comprendiendo claramente las debilidades que hoy en día se tienen en la protección de la información y las oportunidades concernientes al uso de las tecnologías emergentes y disruptivas que posibilites el logro de los objetivos estratégicos de las entidades adscritas.

La metodología DOFA permite identificar las condiciones internas (fortalezas y debilidades) de las entidades en general y las dinámicas externas (oportunidades y amenazas) del entorno. Paralelamente, el análisis PESTEL proporciona una visión integral de los factores que impactan la gestión estratégica de la seguridad

digital, considerando aspectos políticos, económicos, sociales, tecnológicos, ecológicos y legales.

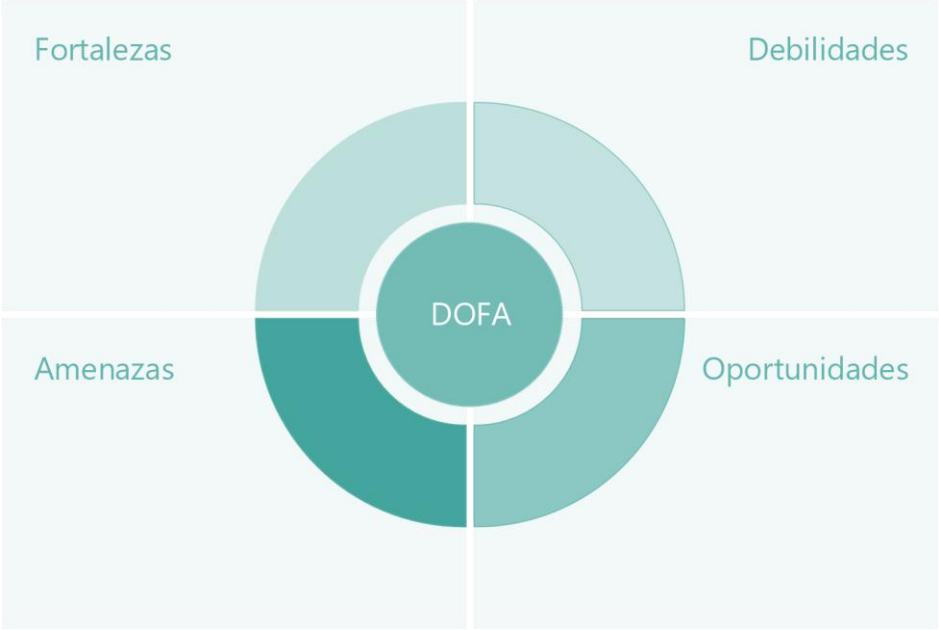

Ilustración 7 Cuadrantes de la matriz DOFA.

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024.

A partir de esta matriz, también se puede desarrollar una matriz cruzada que facilita la definición de estrategias para el plan de seguridad de la información. La matriz cruzada combina elementos de las cuatro áreas para generar el catálogo de iniciativas:

	Factores Positivos	**Factores Negativos**
Factores Internos	F - Fortalezas	D - Debilidades
Factores Externos	O - Oportunidades	A - Amenazas

Tabla 1 Entorno interno y externo para el DOFA

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024.

5. METODOLOGÍA PARA LA ELABORACIÓN DEL ENTREGABLE

Este capítulo explica la metodología utilizada para desarrollar el entregable "PESI SECTORIAL 2025-2028", como el documento que expone el diagnóstico realizado y los proyectos dentro de un marco temporal.

A continuación, se presenta el esquema metodológico recorrido para lograr el presente documento:

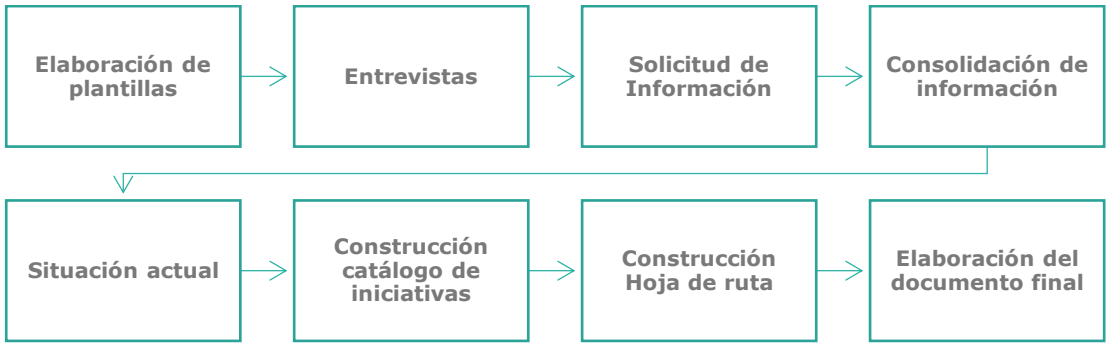

Ilustración 8 Metodología para elaboración del entregable

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024.

Elaboración de plantillas: en esta fase inicial de la construcción del documento PESI se define la estructura documental de los entregables del proyecto y también se consideran las metodologías que se utilizarán.

Entrevistas: se solicita la información que servirá de insumo para construir el PESI, con base en la identificación de las necesidades de información relacionadas con cada una de las fases para de construcción, con lo cual se constituye la línea base del entendimiento y comprensión del funcionamiento operativo de las entidades adscritas.

Solicitud de Información: se solicita la información que servirá de insumo para construir el PESI, con base en la identificación de las necesidades de información con lo cual se establece la línea base del entendimiento y comprensión del cumplimiento en seguridad digital de las entidades sectoriales.

Consolidación de la información: en esta fase del documento PESI se agrupan todas las vulnerabilidades o debilidades encontradas para que más adelante se puedan establecer las iniciativas y proyectos.

Situación actual: conforme a lo establecido en el anexo de especificaciones técnicas de este contrato se realiza el análisis de situación actual o diagnostico el cual será utilizado en etapas posteriores para la construcción de la hoja de ruta.

Construcción catálogo de iniciativas: en esta etapa con base en la información suministrada por medio de las entrevistas y los insumos solicitados se procede a la construcción del catálogo de iniciativas para las entidades sectoriales con su respectiva priorización.

Construcción hoja de ruta: en este paso, con base en el catálogo de iniciativas se estructuran los proyectos considerando su costo y el tiempo requerido de implementación.

Elaboración documento final: una vez realizadas todas las labores expuestas anteriormente se procede a ensamblar el documento PESI Sectorial con base en los dos hitos principales de diagnóstico y de proyección de iniciativas. Este documento tendrá un control de versiones y su respectiva codificación.

6. PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN DEL SECTOR

6.1. Contexto Estratégico de Seguridad de la Información

Este apartado desarrolla el contexto estratégico de seguridad de la información y protección de datos personales y del Sector Salud para el periodo 2024-2028; este análisis representa un componente clave para el fortalecimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), el cual guía la gestión integral de los activos de información bajo custodia de las entidades adscritas.

La elaboración se fundamenta en el análisis detallado de los lineamientos dispuestos en la Estrategia de Seguridad Digital de MinTIC:

Eje 1: Implementación de controles.

Eje 2: Gestión de riesgos.

Eje 3: Gestión de incidentes.

Eje 4: Liderazgo de seguridad de la información.

Eje 5: Concientización.

Ilustración 9 Estrategia de Seguridad Digital

Fuente: https://gobiernodigital.mintic.gov.co/692/w3-article-150511.html

Además, se requiere entender los cinco (5) objetivos de seguridad de la información, que son comunes tanto para el MSPS, como para el Sector Salud:

- Gestionar los activos de información, salvaguardando la información de estos ante cualquier incidente que pueda provocar su destrucción, divulgación, indisponibilidad o uso no compartido.

- Gestionar los riesgos de seguridad de la información aplicando los controles necesarios para cada situación, garantizando la sostenibilidad de las operaciones.

- Fortalecer la cultura de seguridad de la información, brindando concientización y sensibilización permanente a cada colaborador, para enfrentar proactiva y reactivamente las amenazas a las que se exponen en el manejo diario de la información propia y de terceros.

- Establecer mecanismos que permitan mantener la seguridad de la información durante una interrupción de la infraestructura tecnológica que soporta la operación de los servicios ofrecidos por la Entidad.

- Gestionar los eventos e incidentes de seguridad de la información, fortaleciendo la capacidad del Ministerio para hacer frente a las amenazas y ataques informáticos.

A continuación, se presenta la comprensión del entorno de los Ejes Estratégicos frente al cumplimiento de los cinco (5) objetivos de seguridad de la información, comunes para el MSPS como para el Sector Salud:

6.1.1. Implementación de controles.

La implementación de controles de seguridad abarca tanto medidas tecnológicas como administrativas. Los controles tecnológicos pueden incluir la instalación de software de protección contra malware, sistemas de detección de intrusiones y encriptación de datos, entre otros. Los controles administrativos, por otro lado, implican la elaboración de políticas y procedimientos, la gestión de accesos y la realización de auditorías internas. Estos controles son esenciales para asegurar la protección de la información sensible manejada por el MSPS y el Sector, y garantizar la continuidad operativa.

6.1.2. Gestión de riesgos.

La gestión de riesgos en el MSPS y del Sector, se basa en una evaluación continua y sistemática de las amenazas potenciales y la identificación de vulnerabilidades. Este proceso incluye la planificación estratégica para identificar riesgos, la implementación de medidas preventivas y la realización de auditorías regulares para evaluar la efectividad de estos controles. El objetivo es minimizar la probabilidad de incidentes de seguridad y garantizar una respuesta eficaz en caso de que ocurran, protegiendo así la integridad de los sistemas de información.

6.1.3. Gestión de incidentes.

La gestión de incidentes en el MSPS y en el Sector Salud y Protección Social se centra en la identificación, reporte, análisis y resolución de incidentes de seguridad. Un sistema eficiente de gestión de incidentes permite a la entidad responder rápidamente a las amenazas, minimizar su impacto y prevenir futuras ocurrencias. Esto incluye la implementación de un plan de respuesta a incidentes, la capacitación del personal en la detección, atención y reporte de incidentes, y la colaboración con otras entidades para compartir información del entorno.

6.1.4. Liderazgo de seguridad de la información.

El liderazgo en seguridad de la información implica la definición clara de roles y responsabilidades en todos los niveles de la organización. La alta dirección debe promover una cultura de seguridad robusta, asegurando que las políticas y procedimientos sean entendidos y seguidos por todo el personal. Este enfoque holístico no solo garantiza el cumplimiento normativo, sino que también fomenta una cultura organizacional consciente de la seguridad, esencial en la protección de datos sensibles en el Sector Salud y Protección Social.

6.1.5. Concientización.

La concientización en seguridad de la información es un proceso continuo que incluye la formación y capacitación regular de todo el personal. El MSPS implementa programas educativos que promueven el conocimiento de políticas, procedimientos, normas y buenas prácticas en seguridad de la información. Estos programas están diseñados para asegurar que todos los empleados comprendan la importancia de la seguridad y la privacidad de la información y conozcan sus responsabilidades específicas en esta área para el MSPS y el sector.

6.1.6. Contexto Estratégico del Sector Salud y Protección Social

Con el propósito de realizar un análisis más justo y objetivo, se categorizaron las entidades sectoriales en dos grupos: Grupo A, conformado por las entidades que cuentan con un MSPI incipiente y menos maduro; Grupo B, son las entidades que tienen un MSPI más completo y en consecuencia están en un más alto nivel de cumplimiento de los requisitos del MSPI:

Grupo A

- Centro Dermatológico Federico Lleras Acosta.
- Sanatorio de Agua de Dios.
- Sanatorio de Contratación.
- Fondo de Previsión Social del Congreso de la República.
- Fondo del Pasivo Social de Ferrocarriles Nacionales de Colombia.
- Instituto Nacional de Salud.
- Superintendencia Nacional de Salud.
- Instituto de Evaluación Tecnológica en Salud

Grupo B

- Instituto Nacional de Cancerología.
- Instituto Nacional de Medicamentos y Alimentos – INVIMA.
- Administradora de los Recursos del Sistema General de Seguridad Social en Salud- ADRES.

A continuación, se presenta el contexto estratégico del Sector Salud y Protección Social:

En la revisión del Eje Estratégico de Implementación de Controles en cuanto al sector, se debe enfatizar que las entidades del grupo B cuentan con recursos suficientes que les permita adquirir herramientas tecnológicas de control perimetral; en contraposición a las entidades del Grupo B que no tienen los controles mínimos, como tampoco una arquitectura de seguridad definida.

La revisión del Eje Estratégico de Gestión de Riesgos del sector se observa que presenta una situación significativamente crítica en razón a que la gestión de riegos no se hace de manera constante debido a que hay déficit de personal responsable de las actividades de seguridad de la información y protección de datos personales.

En la revisión del Eje Estratégico de Gestión de Incidentes en el Sector, de manera general, la gestión de incidentes se realiza de manera manual, con el agravante de escaso recurso humano que apoye la gestión y herramientas de seguridad que protejan la infraestructura.

La revisión del Eje Estratégico de Liderazgo se evidencia que el MSPS no está ejerciendo las responsabilidades y autoridades apropiadas como cabeza del sector; se espera una gestión más dinámica, que permita desarrollar propuestas o iniciativas, así como, integrar las necesidades del Sector Salud y Protección Social, y responder a ellas de manera integral para que se vea fortalecido el MSPI de las entidades sectoriales en el mismo eje estratégico.

En la revisión del Eje Estratégico de Concientización para el Sector el panorama no es muy prometedor, pues la rotación de los profesionales en seguridad de la información o los pocos recursos asignados, hacen que las campañas no tengan la periodicidad ideal. Integrar campañas sectoriales puede ser una estrategia de bajo costo que permita fortalecer la cultura de la seguridad de la información y protección de datos personales.

6.2. Estado Actual

6.2.1. Análisis del Entorno

Para establecer un análisis del entorno del MSPS y del Sector Salud y Protección Social en el contexto de seguridad de la información, se tuvo en cuenta los lineamentos del MinTIC y la Resolución500 de 2021 frente a los documentos existentes y algunos componentes estructurales del MSPI. Para ello, se

analizaron los documentos entregados, junto con la información obtenida de las entrevistas con los responsables del proceso, para diagnosticar la situación actual de la implementación del MSPI.

Los siguientes son los documentos del MSPI analizados:

- Roles y Responsabilidades
- Políticas de seguridad de la información
- Procesos y procedimientos de seguridad de la información
- Metodología de gestión de activos, inventario de activos de información
- Metodología de gestión de riesgos, matriz de riesgos, plan de tratamiento de riesgos, plan de tratamiento de riegos y controles de seguridad
- Gestión de la cultura de seguridad digital
- Auditoría y revisión del MSPI

Los anteriores aspectos se analizaron en términos de madurez mediante el marco metodológico relacionado en el numeral *4.4 Modelo Gartner de nivel de madurez*, que establece seis (6) niveles:

0-No Existe (0%)

1-Inicial (20%)

2-Repetible (40%)

3-Definido (60%)

4-Administrado (80%)

5-Optimizado (100%)

6.2.1.1. Análisis del Entorno del Sector Salud y Protección Social

Con el propósito de realizar un análisis más justo y objetivo, se categorizaron las entidades sectoriales en dos grupos: Grupo A, conformado por las entidades

que cuentan con un MSPI incipiente y menos maduro; Grupo B, son las entidades que tienen un MSPI más completo y en consecuencia están en un más alto nivel de cumplimiento de los requisitos del modelo:

Grupo A

- Centro Dermatológico Federico Lleras Acosta.
- Sanatorio de Agua de Dios.
- Sanatorio de Contratación.
- Fondo de Previsión Social del Congreso de la República.
- Fondo del Pasivo Social de Ferrocarriles Nacionales de Colombia.
- Instituto Nacional de Salud.
- Superintendencia Nacional de Salud.
- Instituto de Evaluación Tecnológica en Salud

Grupo B

- Instituto Nacional de Cancerología.
- Instituto Nacional de Medicamentos y Alimentos – INVIMA.
- Administradora de los Recursos del Sistema General de Seguridad Social en Salud- ADRES.

6.2.1.2. Documentos del MSPI del Sector Salud y Protección Social

A continuación, se resume el análisis del entorno del Sector, en relación con la revisión de los documentos del MSPI:

Roles y Responsabilidades (Grupo A: 20% - Grupo B: 80%)

La mayoría de las entidades del sector no cuentan con los recursos para conformar un equipo de seguridad de la información. Regularmente la responsabilidad recae en un profesional que hace varias funciones.

Políticas de seguridad de la información (Grupo A: 40% - Grupo B: 60%)

Ninguna entidad del sector cumple con tener todas las políticas mínimas requeridas; la mayoría cumplen con algunos documentos de políticas -o no fueron entregados- y en ocasiones están desactualizados.

Procesos y procedimientos de seguridad de la información (Grupo A: 20% - Grupo B: 60%)

En general, el sector cuenta con la documentación mínima requerida por el MSPI, no obstante, es débil la aplicación y adopción de todos los procesos y procedimientos de seguridad de la información.

Metodología de gestión de activos, inventario de activos de información (Grupo A: 20% - Grupo B: 80%)

Muy pocas entidades del sector cuentan con la metodología de gestión de activos e inventario de activos, o no fue entregado. La gestión se realiza de manera reactiva, sin lineamientos específicos.

Metodología de gestión de riesgos, matriz de riesgos, plan de tratamiento de riesgos, plan de tratamiento de riegos y controles de seguridad (Grupo A: 20% - Grupo B: 60%)

Muy pocas entidades del sector cuentan con documento de lineamientos para la gestión de riesgos; solamente una entidad mostró un plan de tratamiento de riesgos.

Gestión de la cultura de seguridad digital (Grupo A: 20% - Grupo B: 60%)

En general, el sector no cuenta con planes de capacitación y sensibilización en seguridad de la información y protección de datos personales, o no fueron entregados.

Auditoría y revisión del MSPI (Grupo A: 0% - Grupo B: 40%)

La mayoría de las entidades del sector no realiza auditorías al MSPI.

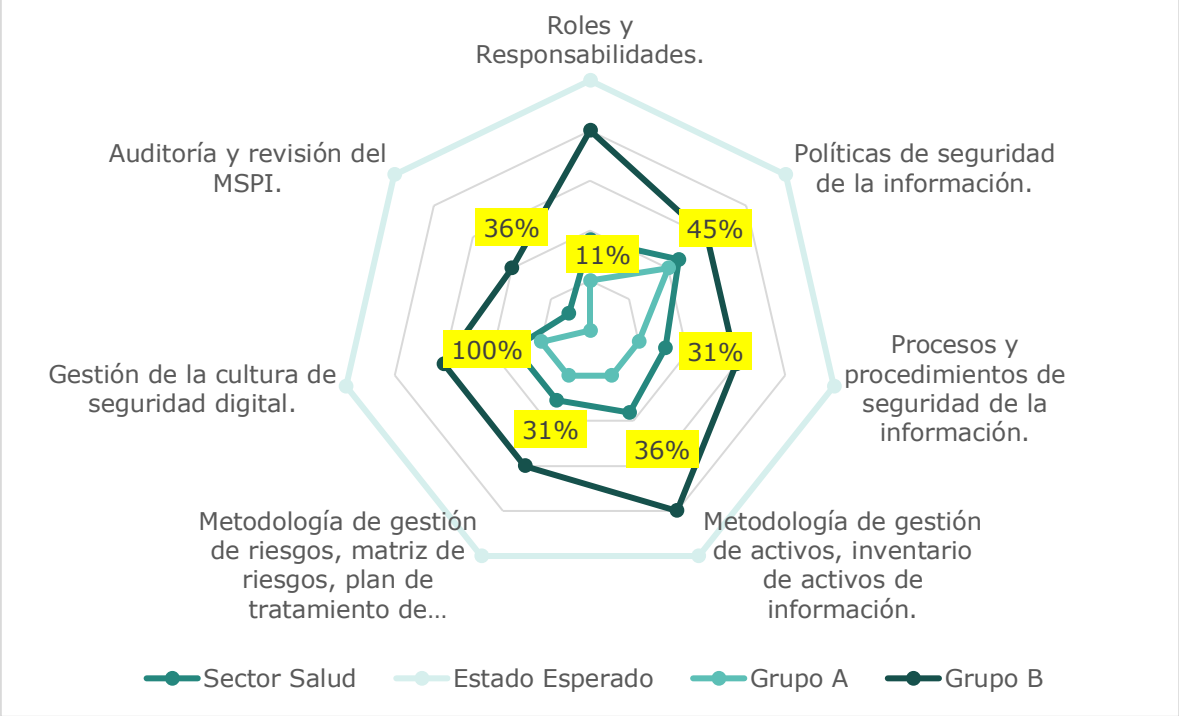

Ilustración 10 Situación actual documentos MSPI del Sector Salud

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

Componentes del MSPI del Sector Salud y Protección Social

A continuación, se resume el análisis del entorno del Sector Salud, en relación con la revisión de los componentes del MSPI:

Arquitectura de seguridad digital (Grupo A: 0% - Grupo B: 0%)

No se aprecia que el sector disponga de una arquitectura de seguridad digital, como resultado de un ejercicio de arquitectura empresarial.

Aseguramiento del modelo de interoperabilidad (Grupo A: 0% - Grupo B: 40%)

Los avances en el modelo de interoperabilidad se identifican por requerimientos del MSPI y particularmente con los ciudadanos que exigen servicios de salud del sector.

Gestión de incidentes de seguridad (Grupo A: 40% - Grupo B: 60%)

Algunas entidades del sector, como ADRES, Centro Dermatológico Federico Lleras, FonFerrocarilles, IETS, INC, INS, INVIMA, Sanatorio Agua de Dios,

Sanatorio de Contratación, Supersalud, no cuentan o no se obtuvo información documentada que respalde la implementación del procedimiento o metodologías de gestión de incidentes, no obstante, se gestionan de manera proactiva, sin seguir lineamientos específicos.

Privacidad de la información y protección de datos personales (Grupo A: 60% - Grupo B: 60%)

El MSPI está implementado en todo el sector de manera incipiente. Se evidenciaron documentos para implementación de controles de seguridad y privacidad de la información en 7 entidades.

Mecanismos de autenticación (Grupo A: 40% - Grupo B: 80%)

Algunas entidades del sector, como Centro Dermatológico Federico Lleras, FonFerrocarilles, FonPRECON, INVIMA, Sanatorio Agua de Dios, Sanatorio de Contratación, Supersalud, no cuentan o no se obtuvo información documentada que respalde la implementación de lineamientos de autenticación.

Retención y destrucción final de información (Grupo A: 40% - Grupo B: 60%)

Algunas entidades del sector, como ADRES, Centro Dermatológico Federico Lleras, FonFerrocarilles, IETS, INC, INS, INVIMA, Sanatorio Agua de Dios, Sanatorio de Contratación, Supersalud, no cuentan o no se obtuvo información documentada que respalde la implementación del procedimiento de borrado seguro, no obstante, ejecutan procedimientos básicos de borrado.

Aseguramiento del proceso de desarrollo de software (Grupo A: 20% - Grupo B: 60%)

Algunas entidades del sector, como ADRES, Centro Dermatológico Federico Lleras, FonFerrocarilles, FonPRECON, IETS, INC, INS, INVIMA, Sanatorio Agua de Dios, Sanatorio de Contratación, Supersalud, no cuentan o no se obtuvo información documentada que respalde la implementación del procedimiento de desarrollo seguro.

Gestión segura de terceros y colaboradores (Grupo A: 40% - Grupo B: 60%)

Algunas entidades del sector, como Centro Dermatológico Federico Lleras, FonFerrocarilles, FonPRECON, IETS, INC, INS, INVIMA, Sanatorio Agua de Dios, Sanatorio de Contratación, Supersalud, no cuentan o no se obtuvo información documentada que respalde la implementación del procedimiento de gestión segura de terceros o proveedores.

Gestión de Continuidad de Recuperación de desastres (Grupo A: 20% - Grupo B: 40%)

Algunas entidades del sector, como ADRES, FonFerrocarilles, INS, INVIMA, Sanatorio Agua de Dios, Sanatorio de Contratación, Supersalud, no cuentan o no se obtuvo información documentada que respalde la implementación del procedimiento o planes de continuidad o planes de recuperación de desastres.

Gestión de vulnerabilidades (Grupo A: 20% - Grupo B: 60%)

Algunas entidades del sector, como ADRES, Centro Dermatológico Federico Lleras, IETS, INC, INS, INVIMA, Sanatorio Agua de Dios, Sanatorio de Contratación, Supersalud, no cuentan o no se obtuvo información documentada que respalde la implementación del procedimiento de gestión de vulnerabilidades, no obstante, algunas lo realizan con herramientas análisis de código. El sector no cuenta con herramientas de monitoreo.

Monitoreo de seguridad y correlación de eventos (Grupo A: 20% - Grupo B: 20%)

De ninguna entidad del sector se obtuvo información documentada que respalde la implementación del procedimiento de monitoreo, además, el sector no cuenta con herramientas de monitoreo.

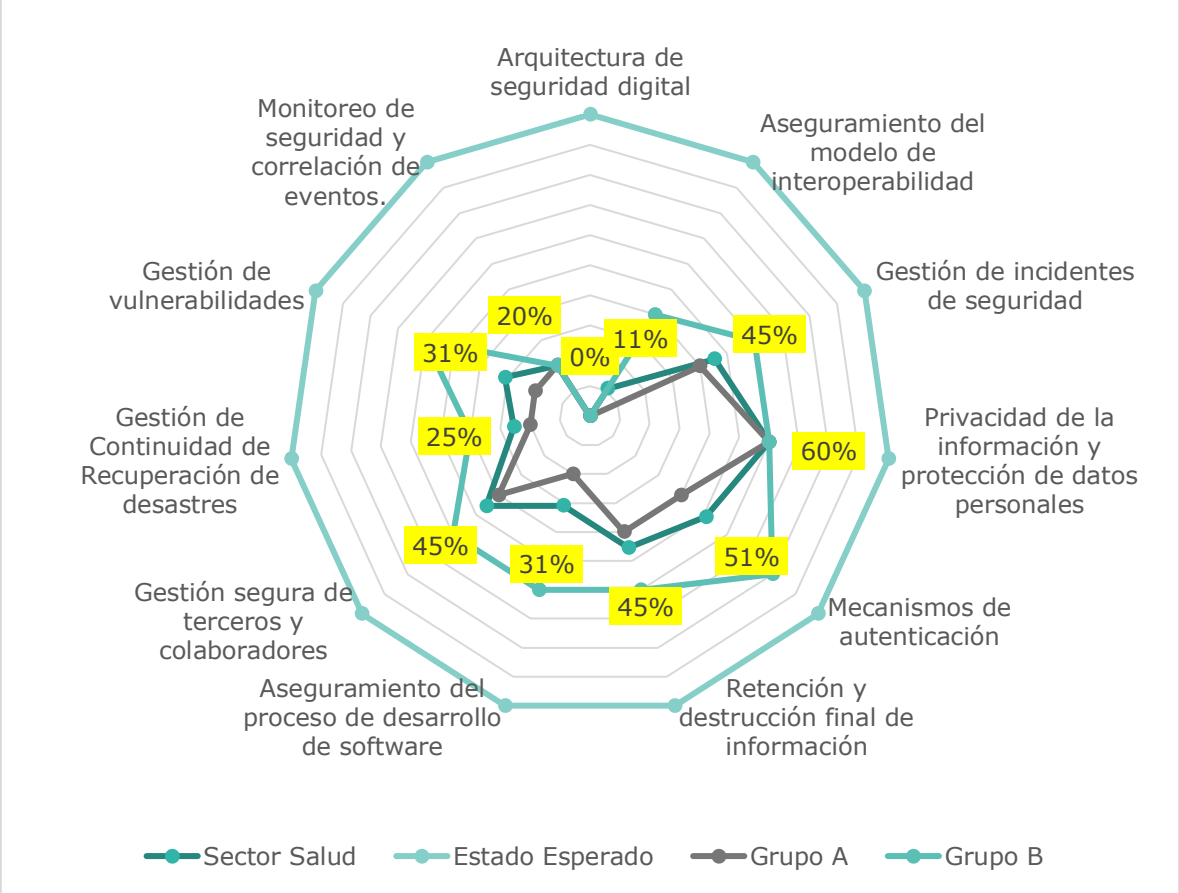

Ilustración 11 Situación actual componentes MSPI del Sector Salud

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

Análisis DOFA del Sector Salud y Protección Social

Debilidades

Debido a recursos humanos técnicos limitados, la infraestructura tecnológica puede no estar completamente actualizada o contar con los componentes de seguridad suficientes, lo cual limita la capacidad del sector salud para proteger adecuadamente la información frente a amenazas cibernéticas avanzadas. Por otra parte, La interoperabilidad entre sistemas de salud (sector) es insuficiente, lo cual dificulta una gestión centralizada y segura de los datos de salud y personales de los ciudadanos.

Oportunidades

Existe una amplia oferta de capacitaciones virtuales nacionales e internacionales en temas de ciberseguridad que pueden ser aprovechadas por el sector salud.

Además, la evolución de nuevos marcos de trabajo, normatividad y buenas prácticas en materia de seguridad de la información y digital, están al alcance para que sean validadas y adoptadas por el sector.

Fortalezas

El sector salud cuenta con el apoyo permanente del MSPS en materia de seguridad de la información y protección de datos personales mediante la presentación de proyectos de tecnología.

Amenazas

Los sistemas de información en salud requieren integración entre distintas entidades, lo cual puede aumentar el riesgo de brechas de seguridad. MSPS debe asegurar la interoperabilidad con el sector salud sin comprometer la seguridad.

Análisis PESTEL del Sector Salud y Protección Social

Político

La legislación en Colombia exige la protección de los datos personales y la adopción de la ciberseguridad en las instituciones públicas, especialmente en aquellas que manejan información sensible como el sector salud. Por otra parte, la falta de estabilidad política y la insuficiente capacidad del gobierno de promover políticas de ciberseguridad coherentes afecta la continuidad de los programas de protección de datos. Los cambios de administración pueden influir en las prioridades y en los presupuestos asignados.

Económico

Debido a recursos técnicos limitados, la infraestructura tecnológica puede no estar completamente actualizada o no contar con los componentes de seguridad suficientes, lo cual limita la capacidad del sector salud para proteger adecuadamente la información frente a amenazas cibernéticas avanzadas.

Social

La confianza de los ciudadanos en el manejo de sus datos personales es crucial para el sector salud, por tanto, escándalos o violaciones de seguridad pueden afectar la reputación de las entidades y disminuir la cooperación ciudadana y su percepción de seguridad del sector en general.

Tecnológico

Las iniciativas del sector en torno a temas de seguridad de la información y protección de datos personales deben pasar primero por el MSPS para valorar su viabilidad, esta situación hace lentos los procesos de inversión en tecnología.

Ecológico

No existe una cultura de apagado de equipos durante la noche y fines de semana en las dependencias de algunas entidades del sector salud para propender por el ahorro energético y uso apropiado de equipos.

Legal

Las políticas internas de cada una de las entidades del sector salud deben alinearse con las políticas del MSPS para garantizar un manejo estandarizado de la seguridad de la información.

6.2.2. Diagnóstico

Para establecer un diagnóstico de la situación actual del Sistema de Gestión de Seguridad de la Información del Sector Salud, se llevó a cabo una evaluación comparativa con los requisitos de la norma ISO 27001:2022 y los lineamientos del Modelo de Seguridad y Privacidad del MinTIC. Para ello, se analizaron los documentos entregados por las entidades del sector y se realizaron entrevistas a los responsables del proceso, lo que permitió obtener una visión integral de la situación actual. Es importante resaltar que no todas las entidades entregaron documentación para este análisis. El informe en donde se encuentra el análisis de la información entregada por las entidades del sector es "Análisis del Modelo de Gobierno y Operación".

Para la elaboración del diagnóstico se tuvieron en cuenta los siguientes documentos:

- Informe análisis y comprensión de seguridad
- Análisis del Modelo de Gobierno y Operación de MSPI
- Análisis DOFA_ PESTEL
- Análisis del Entorno del Ministerio de Salud y Protección Social y el Sector
- Análisis y comprensión de hallazgos y oportunidades de mejora.
- Diagnóstico de seguridad digital Institucional y sectorial.

Los lineamientos del MSPI que se evaluaron fueron los siguientes.

- 7.1.1 Comprensión de la Organización y de su Contexto
- 7.1.2 Necesidades y Expectativas de los Interesados
- 7.1.3 Definición del Alcance del MSPI
- 7.2.1 Liderazgo y Compromiso
- 7.2.2 Política de Seguridad y Privacidad de la Información
- 7.2.3 Roles y Responsabilidades
- 7.3.1 Identificación de Activos de Información e Infraestructura Crítica
- 7.3.2 Valoración de los Riesgos de Seguridad de la Información
- 7.3.3 Plan de Tratamiento de los Riesgos de Seguridad de la Información
- 7.4.1 Recursos
- 7.4.2 Competencia, Toma de Conciencia y Comunicación
- 8.2 Evaluación de Riesgos
- 9.1.1 Seguimiento, Medición, Análisis y Evaluación
- 9.1.2 Auditoría Interna
- 10.1 Mejora

Así mismo, se revisaron los siguientes controles clave del MSPI

- Procesos y procedimientos de seguridad de la información
- Arquitectura de seguridad digital.
- Aseguramiento del modelo de interoperabilidad.
- Gestión de incidentes de seguridad.
- Privacidad de la información y protección de datos personales.
- Mecanismos de autenticación.
- Retención y destrucción final de información.
- Aseguramiento del proceso de desarrollo de software.
- Gestión segura de terceros y colaboradores.
- Gestión de Continuidad de Recuperación de desastres.
- Gestión de vulnerabilidades.
- Monitoreo de seguridad y correlación de eventos.

6.2.3. Acciones de Mejora Controles Claves de Seguridad Digital

A continuación, se presentan las principales acciones de mejora resultado de los hallazgos encontrados durante las actividades relacionadas con el análisis de la situación sectorial. Estas acciones de mejora están plenamente alineadas con los proyectos definidos en la hoja de ruta.

6.2.3.1. Gobierno de Seguridad

Revisar y modernizar el modelo de gobierno sectorial para conseguir una protección homogénea de la información de los ciudadanos y una articulación adecuada con las entidades del sector. Este modelo de gobierno debe poner especial atención a nuevas tecnologías, nuevos servicios de las entidades, necesidades de los ciudadanos, colaboración interinstitucional, normalización de procesos, ejecución de pruebas conjuntas y estándares de interoperabilidad.

El gobierno sectorial que se propone busca homogenizar tanto las adquisiciones de nuevas tecnologías que se hagan, así como las políticas, procedimientos, estándares del modelo de seguridad digital. Unificar las estrategias de seguridad digital desde el punto de vista sectorial se reflejará en una mejora tanto en eficacia como en eficiencia. Esto incluye, por ejemplo, la unificación de los eventos e incidentes de seguridad de la información sectorial e institucional.

6.2.3.2. Arquitectura de Seguridad

Realizar la identificación de riesgos de seguridad a partir del ejercicio de Arquitectura empresarial, para mejorar la alineación estratégica de las entidades del sector, de acuerdo con las capacidades en seguridad de la información. Así mismo, desarrollar y mantener actualizados todos los artefactos del dominio de seguridad de Arquitectura Empresarial de acuerdo con los requerimientos del MinTIC. Por último, es necesario incluir capacitaciones y competencias en el dominio de seguridad de Arquitectura Empresarial para el recurso humano del grupo de seguridad de las entidades.

La arquitectura de seguridad de las entidades sectoriales debe estar alineadas con las directrices emitidas por el MSPS y deben considerar al menos los siguientes puntos:

- Diseñar la estrategia general de seguridad de la información alineada con los objetivos estratégicos de la Entidad y los lineamientos emitidos por el MSPS.
- Gestionar los presupuestos de inversión en tecnologías para mejor la seguridad digital con el apoyo del MSPS
- Gestionar los proyectos de mejora de la seguridad digital
- Gestionar todo lo relacionado con las vulnerabilidades sobre los sistemas de información y componentes tecnológicos
- Coordinar a todos los responsables de la seguridad de la información en torno a una meta compartida y de acuerdo con las políticas establecidas por el MSPS
- Garantizar el cumplimiento de las leyes y reglamentos aplicables para el sector.
- Apoyar la interoperabilidad entre todos los componentes que supervisan la seguridad de la información a nivel sectorial.
-

6.2.3.3. Herramientas de Seguridad

Los sistemas de gestión de las entidades sectoriales debe propender por la implementación de herramientas de seguridad de la información como resultado de una evaluación de riesgos y de acuerdo con las necesidades actuales, como desarrollo seguro, cifrado de bases de datos, gestión de riesgos, sensibilización y borrado seguro y necesidades futuras que se presente con los desarrollos actuales y futuros de la inteligencia artificial que por un lado nos ofrece algoritmos para que el software implementado sea más seguro y la vez se pueda establecer una barrera de protección contra nuevos tipos de ataques con tecnologías emergentes.

Cuando se trate de la implementación de herramientas de seguridad es indispensable que estas a su vez cumplan con las mejores prácticas a nivel internacional y que permitan la interoperabilidad con otro tipo de herramientas para poder contar con una gestión centralizada y que estos nuevos instrumentos actúen en conjunto con los controles actuales. Finalmente, la capacitación sobre estas herramientas debe ser consistente y completa para que se puede así obtener el mayor provecho de estas para evitar incidentes de seguridad que afecten la operación y la información del MSPS.

6.2.3.4. Servicios de Seguridad

El propósito de la identificación de los servicios de seguridad digital es proporcionar una fuente única de información coherente sobre ellos y garantizar que esta información esté disponible para consulta de partes interesadas.

La gestión de catálogos de servicios de seguridad digital incluye un conjunto continuo de actividades relacionadas con la publicación, edición, control y actualización de la información de estos servicios.

Las entidades sectoriales deben avanzar en este propósito a medida que se mejoren los niveles de madurez en los controles que se implementen en seguridad digital. Algunos ejemplos de servicios de seguridad digital son:

Gestión de Incidentes de Seguridad

Detectar y combatir intrusiones y minimizar los daños colaterales o directos como consecuencia de la explotación de una vulnerabilidad.

Apoyo en la implementación de controles de Seguridad

Se busca que con este tipo de controles tanto técnicos como administrativos asegurar la confidencialidad, la integridad, la seguridad y la disponibilidad de los activos de información.

Gestión de vulnerabilidades

Se busca con esta iniciativa que todos los mecanismos de seguridad sean objeto de pruebas frecuentes para validar su efectividad.

Auditorías de Seguridad

Revisar que las medidas y procedimientos de seguridad sean efectivas a todo momento y que sobre ellas se realicen mejoras continuas.

6.2.3.5. Políticas

Las entidades del sector deben:

- Elaborar, aprobar y aplicar políticas de seguridad sectoriales.
- Optimizar las políticas de cada entidad alineándolas con las sectoriales una vez creadas y ajustarlas para atender sus necesidades específicas. Se deben crear Políticas de protección contra malware y servicios en la nube.

6.2.3.6. Capacidad de Recursos

- Las entidades deben formular proyectos de tecnología y seguridad de la información como resultado de un análisis de riesgos y presentarlos al MSPS para su financiación.
- Dimensionar la capacidad de recurso humano necesaria para implementar y operar la totalidad de procesos del SGSI en las entidades, esta capacidad se debe presentar al MSPS para su gestión.

6.2.3.7. Conocimientos en Seguridad de la Información

Implementar un plan de capacitaciones a todo nivel, que incluya en especial, la alta dirección de cada entidad y otros interesados que impacten el gobierno del SGSI. Se deben realizar capacitaciones de forma continua y a todos los interesados en temas regulatorios, nuevas tecnologías y servicios del SGSI de la entidad. Se puede coordinar con el MSPS para recibir su apoyo en ese aspecto, de tal manera que se maximicen los recursos.

6.2.3.8. Seguridad de la Información en la Continuidad De Negocio.

Las entidades deben elaborar un plan de continuidad y probarlo periódicamente, que incluya los procesos más críticos de la entidad. Como resultado de este ejercicio es posible desarrollar un DRP sectorial para la maximización de recursos.

6.2.3.9. Seguridad de la Información en Acuerdos con Terceros

Las entidades del sector deben revisar e implementar acuerdos con terceros que incluyan entre otros:

- Colaboración para la contención y gestión de incidentes;
- Auditorías;
- Derechos de autor;
- Acuerdos de confidencialidad;
- Acuerdos de protección para intercambios de información y
- Protección de datos personales entre otros;

Para los contratistas que trabajan directamente en funciones de las entidades del sector, se debe solicitar en los contratos, la obligatoriedad de la toma de capacitaciones y aplicación de controles definidos en los SGSI.

6.2.3.10. Controles de los Procesos de Seguridad de la Información

Las entidades deben crear cuando sea necesario puntos de control y generar a partir de ellos reportes, para validar el funcionamiento esperado de los procesos del SGSI, entre ellos:

- Procedimiento de Cifrado de Información
- Procedimiento de Monitoreo y Detección.
- Procedimiento de Respaldo y Restauración.
- Procedimiento para la gestión de incidentes de seguridad.
- Procesos y herramientas para la gestión de la configuración.
- Retención y destrucción final de la información.
- Procedimiento de adquisición, desarrollo y mantenimiento de sistemas de información (desarrollo seguro)

6.2.3.11. Protección de los Datos Personales

Las entidades deben verificar y actualizar periódicamente los activos de información en donde se encuentren datos personales y valorar los riesgos nuevamente. Así mismo, establecer puntos de verificación de la aplicación de controles de protección de datos personales en las diferentes regiones del país. De otra parte, socializar con la ciudadanía el porqué de la existencia de estos controles. Muy importante revisar y ajustar los controles para la protección de datos personales cuando se intercambia información entre entidades.

6.2.3.12. Plan de Mejora

Las entidades del sector deben elaborar y desarrollar un plan de mejora que tenga en cuenta revisiones internas, revisiones independientes, no conformidades y oportunidades de mejora reportadas por funcionarios y contratistas, garantizado la implementación completa del MSPI.

6.2.3.13. Gestión de vulnerabilidades y gestión de incidentes

Se debe establecer un marco de gestión de incidentes unificado y articulado para todas las entidades del sector, considerando las necesidades tecnológicas y operativas de cada una; así mismo, se debe establecer un marco de gestión de vulnerabilidades con las mismas características.

6.2.4. Análisis de Maduración

Con el propósito de realizar un análisis más objetivo, se categorizaron las entidades sectoriales en dos grupos: Grupo A, conformado por las entidades que cuentan con menos recursos, y por lo tanto poseen herramientas de seguridad menos robustas; Grupo B, son las entidades que tienen un MSPI más completo, por contar con más recursos.

Grupo	ENTIDADES
A	• Centro Dermatológico Federico Lleras Acosta. • Sanatorio de Agua de Dios • Sanatorio de Contratación • Fondo de Previsión Social del Congreso de la República • Fondo del Pasivo Social de Ferrocarriles Nacionales de Colombia. • Instituto Nacional de Salud • Superintendencia Nacional de Salud • Instituto de Evaluación Tecnológica en Salud
B	• Instituto Nacional de Cancerología • Instituto Nacional de Medicamentos y Alimentos – INVIMA • Administradora de los Recursos del Sistema General de Seguridad Social en Salud- ADRES.

Tabla 2 Categorizaron las Entidades Sectoriales

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

La metodología para identificar el estado actual de los principales lineamientos y controles clave de las entidades del sector salud, está completamente alineada con las directrices del MinTIC y hacen uso del marco de referencia para niveles de madurez establecido por Gartner Inc. A continuación, se presentan los niveles de madurez y su descripción.

NIVEL DE MADUREZ	CALIFICACIÓN	DESCRIPCIÓN DEL NIVEL
0 - Nulo	0%	No se identifica evidencia de cumplimiento ni adopción. Se caracteriza por actividades improvisadas, indocumentadas e impredecibles. Sin procesos formales para gestionar la seguridad de la información.
1 - Inicial	20%	Hay una evidencia de que la organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican. Se ha identificado la necesidad de implementar un modelo de Seguridad de la Información y se gestionan algunas actividades de seguridad.
2 - Repetible	40%	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
3 - Definido	60%	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada. El modelo de seguridad y privacidad de la información se tiene documentado, estandarizado y aprobado por la dirección. Todos los requisitos se encuentran documentados, aprobados, implementados y actualizados.
4 - Administrado	80%	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente. Se cuenta con métricas, indicadores y se realizan auditorías al modelo de seguridad y privacidad de la información, recolectando información para establecer la efectividad de los controles y el SGSI.
5 - Optimizado	100%	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Tabla 3 Niveles de maduración Gartner

Fuente: Gartner

6.2.4.1. Análisis de Maduración: Valoración Frente a los Lineamientos del MSPI Grupo A

En la revisión frente a los lineamientos del MSPI se encontraron en un estado de implementación "Nulo e Inicial" los siguientes lineamientos:

- 7.2.1 Liderazgo y Compromiso
- 7.2.3 Roles y Responsabilidades.
- 7.3.1 Identificación de Activos de Información e Infraestructura Crítica.
- 7.3.2 Valoración de los Riesgos de Seguridad de la Información.
- 7.4.1 Recursos.
- 7.4.2 Competencia, Toma de Conciencia y Comunicación.
- 8.2 Evaluación de Riesgos.
- 9.1.1 Seguimiento, Medición, Análisis y Evaluación.
- 9.1.2 Auditoría Interna.

Las entidades del grupo A, no realizan o no se obtuvo respaldo documental suficiente que soportara la realización de las actividades de cada uno de esos lineamientos.

Como principales fortalezas de este grupo, calificadas en "Definido" se encuentran los siguientes lineamientos:

- 7.1.1 Comprensión de la Organización y de su Contexto
- 7.1.2 Necesidades y Expectativas de los Interesados.
- 7.1.3 Definición del Alcance del MSPI.
- 7.3.3 Plan de Tratamiento de los Riesgos de Seguridad de la Información.

Indicando que las entidades del grupo A, realizan las actividades para los anteriores lineamientos y las comunican, pero es posible que les falte algunos elementos, tales como: monitorear, medir el cumplimiento de los procedimientos o tomar medidas de acción donde los procesos no estén funcionando eficientemente.

A continuación, se presenta el resumen diagnóstico en una gráfica radial del resultado frente a los lineamientos del MSPI del Grupo A.

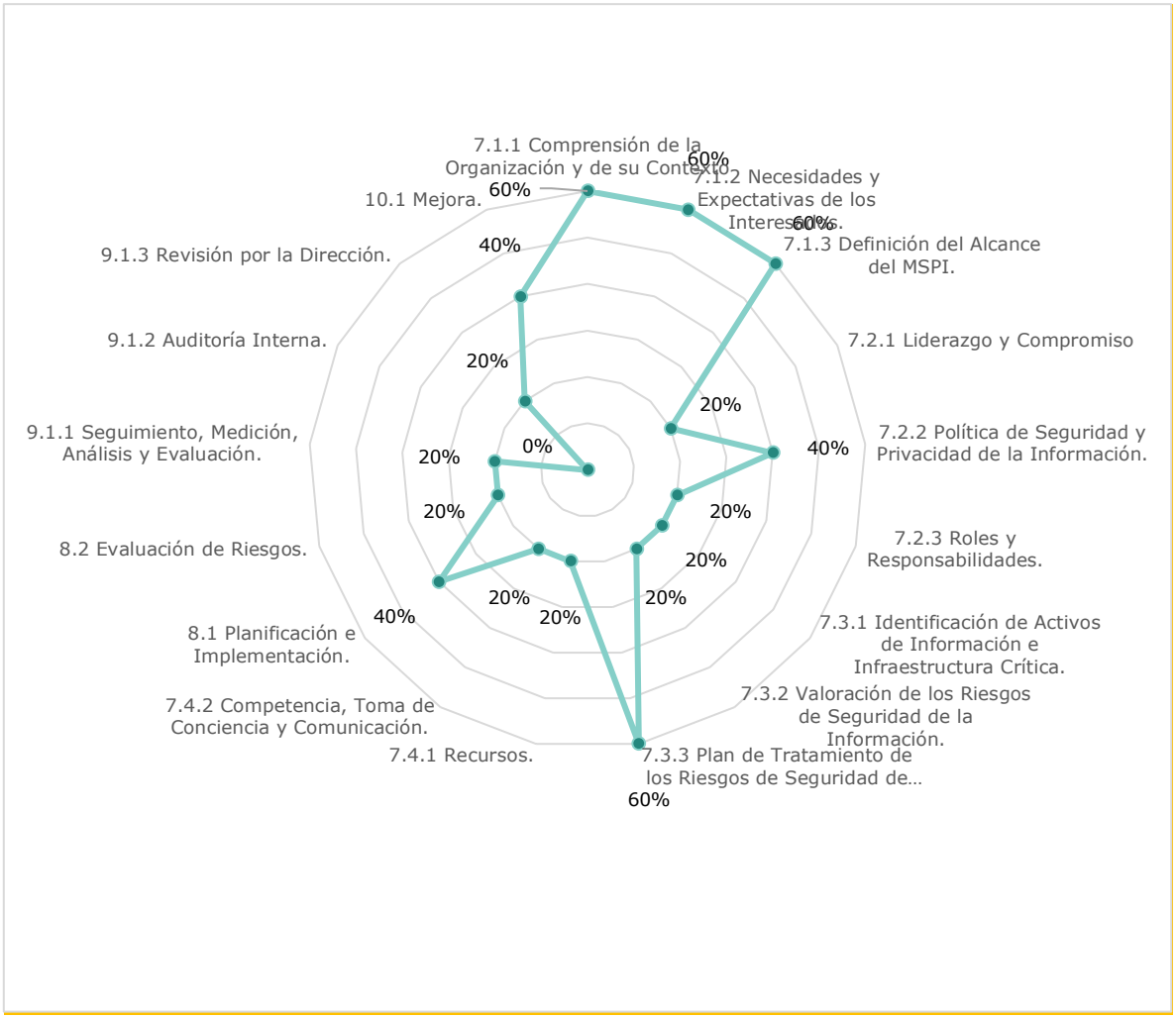

Ilustración 12 Diagnóstico Sectorial Lineamientos MSPI -Grupo A

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

6.2.4.2. Análisis de Maduración: Valoración frente a los Lineamientos del MSPI Grupo B

En la revisión frente a los lineamientos del MSPI se encontraron en un estado de implementación repetible los siguientes lineamientos:

- 9.1.2 Auditoría Interna.

Las entidades del grupo B, no tienen lineamientos con un estado de madurez nulo o inicial, su valoración más baja se encuentra en estado "Repetible".

Como principales fortalezas de este grupo, calificadas en "Administrado" se encuentran los siguientes lineamientos:

- 7.1.1 Comprensión de la Organización y de su Contexto
- 7.1.2 Necesidades y Expectativas de los Interesados.
- 7.1.3 Definición del Alcance del MSPI.
- 7.2.1 Liderazgo y Compromiso
- 7.2.3 Roles y Responsabilidades.
- 7.3.1 Identificación de Activos de Información e Infraestructura Crítica.
- 7.3.3 Plan de Tratamiento de los Riesgos de Seguridad de la Información.
- 7.4.1 Recursos.
- 8.1 Planificación e Implementación.
- 10.1 Mejora.

Indicando que las entidades del grupo B, realizan las actividades para los anteriores lineamientos, que cumplen con el monitoreo, medición del cumplimiento de los procedimientos y se toman las medidas de acción necesarias en donde los procesos no estén funcionando eficientemente

A continuación, se presenta el resumen diagnóstico en una gráfica radial del resultado frente a los lineamientos del MSPI del Grupo B.

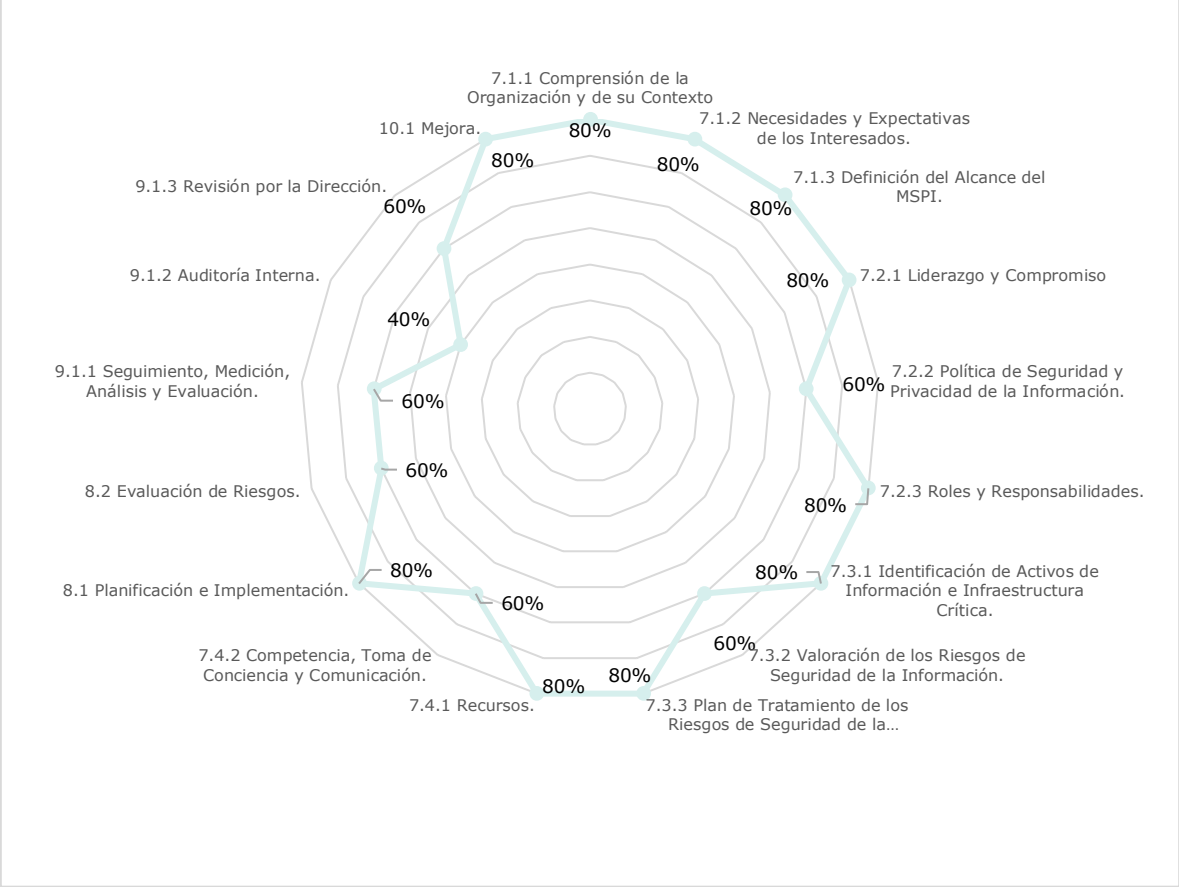

Ilustración 13 Diagnóstico Sectorial Lineamientos MSPI -Grupo B

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

6.2.4.3. Análisis de Maduración: Valoración Frente a Controles Clave de Seguridad de la Información del Grupo A.

En la revisión frente a los controles clave del MSPI se encontraron en un estado de implementación nulo e inicial los siguientes:

- Arquitectura de seguridad digital.
- Aseguramiento del modelo de interoperabilidad.
- Aseguramiento del proceso de desarrollo de software.
- Gestión de Continuidad de Recuperación de desastres.
- Gestión de vulnerabilidades.
- Monitoreo de seguridad y correlación de eventos.

Las entidades del grupo A, no realizan o no se obtuvo respaldo documental suficiente que soportara la realización de las actividades de cada uno de esos controles clave de seguridad.

Como principales fortalezas de este grupo, calificadas en "Definido" se encuentran los siguientes controles clave:

- Privacidad de la información y protección de datos personales.

Indicando que las entidades del grupo A, realizan la actividad para el anterior control clave y las comunican, pero es posible que les falte algunos elementos tales como: monitorear, medir el cumplimiento de los procedimientos o tomar medidas de acción donde los procesos no estén funcionando eficientemente.

A continuación, se presenta el resumen diagnóstico en una gráfica radial del resultado frente a los controles clave del MSPI del Grupo A.

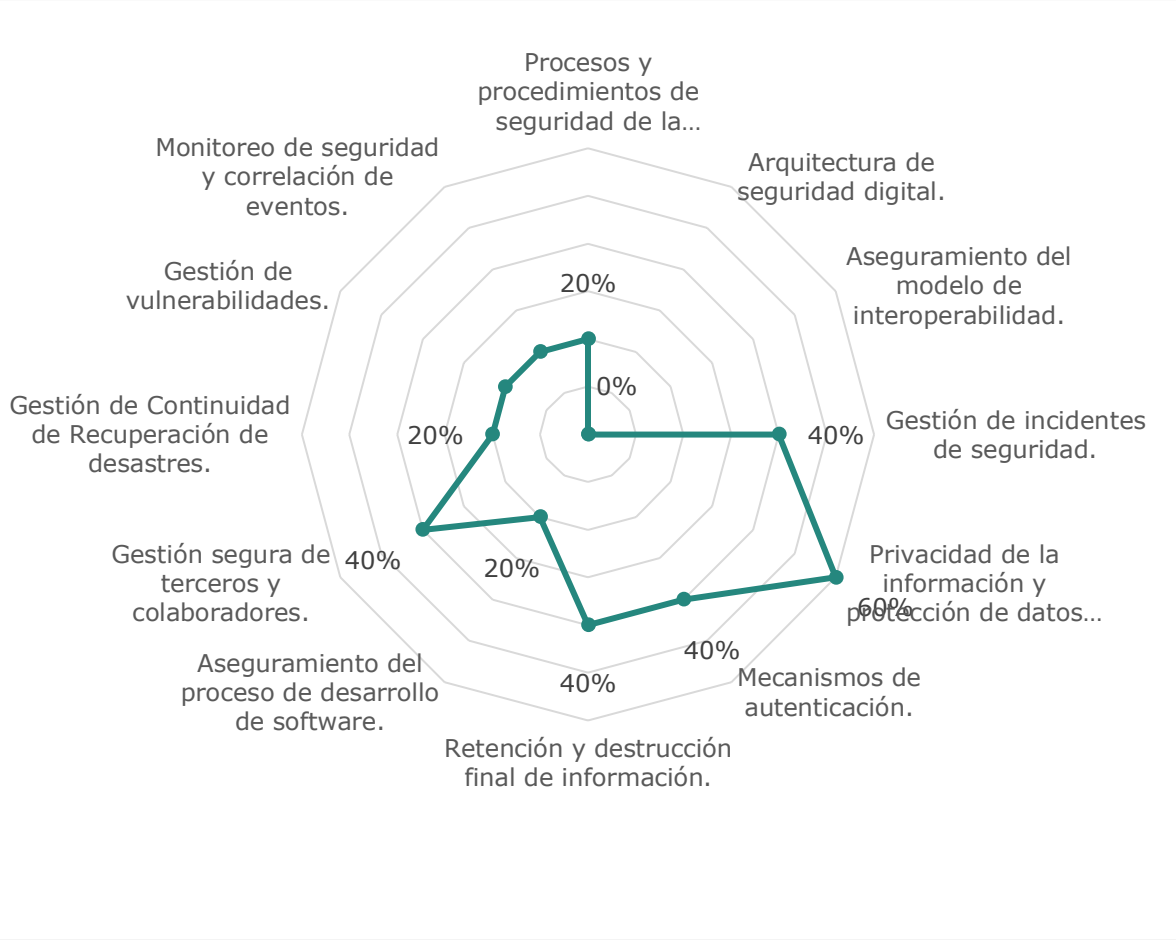

Ilustración 14 Diagnóstico Sectorial Controles Clave -Grupo A

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

6.2.4.4. Análisis de Maduración: Valoración Frente Controles Clave de Seguridad de la Información del Grupo B.

En la revisión frente a los controles clave del MSPI se encontraron en un estado de implementación nulo e inicial los siguientes:

- Arquitectura de seguridad digital.
- Monitoreo de seguridad y correlación de eventos.

Las entidades del grupo B, no realizan o no se obtuvo respaldo documental suficiente que soportara la realización de las actividades de cada uno de esos controles clave.

Como principales fortalezas de este grupo, calificadas en "Definido" se encuentran los siguientes controles claves:

- Procesos y procedimientos de seguridad de la información
- Gestión de incidentes de seguridad.
- Privacidad de la información y protección de datos personales.
- Retención y destrucción final de información.
- Aseguramiento del proceso de desarrollo de software.
- Gestión segura de terceros y colaboradores.
- Gestión de vulnerabilidades.

Indicando que las entidades del grupo B, realizan las actividades para los anteriores controles clave y las comunican, pero es posible que les falte algunos elementos, como: monitorear, medir el cumplimiento de los procedimientos o tomar medidas de acción donde los procesos no estén funcionando eficientemente.

Como principales fortalezas de este grupo, calificadas en "Administrado" se encuentra el siguiente control clave:

- Mecanismos de autenticación.

A continuación, se presenta el resumen diagnóstico en una gráfica radial del resultado frente a los controles clave del MSPI del Grupo B.

Ilustración 15 Diagnóstico Sectorial Controles Clave -Grupo B

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

Para ver el detalle de las observaciones frente a los todos los aspectos de los lineamientos del MSPI y frente a los controles clave, remítase a los documentos:

- Análisis y comprensión de hallazgos y oportunidades de mejora.
- Diagnóstico de seguridad digital Institucional y sectorial.

6.3. Estrategias

6.3.1. Iniciativas vs Objetivos Estratégicos SI

A continuación, se presenta la relación entre Objetivos e Iniciativas para el Plan Estratégico de Seguridad de la Información del Ministerio de Salud y Protección Social

El Ministerio de Salud y Protección Social ha definido cinco objetivos estratégicos clave para fortalecer la seguridad de la información dentro de su infraestructura. Estos objetivos buscan gestionar eficazmente los activos de información, administrar los riesgos de seguridad, fomentar una cultura de seguridad robusta, establecer mecanismos para mantener la seguridad durante interrupciones tecnológicas y gestionar eventos e incidentes de seguridad de la información. Para alcanzar estos objetivos, se han diseñado diversas iniciativas estratégicas que abordan de manera integral cada uno de estos aspectos.

El primer objetivo, "Gestionar los activos de información" (OBJ1), se enfoca en salvaguardar la información ante cualquier incidente que pueda causar su destrucción, divulgación, indisponibilidad o uso no autorizado. Para cumplir con este objetivo, se han implementado varias iniciativas. La iniciativa INI002, que consiste en la adquisición de los recursos necesarios para la implementación de los servicios de un CSIRT Sectorial, juega un papel fundamental al anticipar y monitorizar amenazas cibernéticas sobre la infraestructura TI del sector. Asimismo, la iniciativa INI003, que implica la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) para todos los procesos de negocio, proporciona un marco integral que refuerza la gestión y protección de los activos de información. Además, la iniciativa INI006, dedicada a implementar un modelo de cifrado para las bases de datos que contienen información personal y sensible, asegura la confidencialidad e integridad de los datos críticos. La iniciativa INI009, que desarrolla una estrategia para la clasificación de activos de información y datos personales, facilita una gestión eficiente y priorización de los recursos según la criticidad de los activos, contribuyendo significativamente a la protección de la información.

El segundo objetivo, "Gestionar los riesgos de seguridad de la información" (OBJ2), se centra en aplicar los controles necesarios para cada situación, garantizando la sostenibilidad de las operaciones. Las iniciativas INI002, INI003, INI006, INI009 e INI010 están alineadas con este objetivo, ya que todas ellas contribuyen a identificar, evaluar y mitigar riesgos. La implementación del CSIRT sectorial y el modelo MSPI proporcionan mecanismos robustos para la gestión de riesgos, mientras que las iniciativas INI006 y INI010 enfocan esfuerzos específicos en la protección de datos y la gestión de riesgos de seguridad, respectivamente. Además, la clasificación de activos mediante INI009 permite

una evaluación más precisa de los riesgos asociados a cada activo de información.

El tercer objetivo, "Fortalecer la cultura de seguridad de la información" (OBJ3), busca brindar concientización y sensibilización permanente a los colaboradores para enfrentar de manera proactiva y reactiva las amenazas en el manejo diario de la información. Las iniciativas INI002, INI003, INI004 e INI008 son fundamentales para este objetivo. La implementación del CSIRT y el modelo MSPI no solo fortalecen la infraestructura de seguridad, sino que también promueven una cultura organizacional orientada a la seguridad. La iniciativa INI004, que establece un equipo de trabajo especializado para la gestión de la seguridad de la información, asegura una coordinación efectiva de las actividades relacionadas con la seguridad, mientras que la iniciativa INI008, enfocada en diseñar una campaña orientada a la cultura de seguridad, sensibiliza a todos los niveles de la organización sobre la importancia de proteger la información y adoptar buenas prácticas de seguridad.

El cuarto objetivo, "Establecer mecanismos para mantener la seguridad durante interrupciones tecnológicas" (OBJ4), tiene como propósito garantizar la continuidad operativa y la resiliencia ante interrupciones en la infraestructura tecnológica. Las iniciativas INI002, INI003, INI004 e INI008 contribuyen directamente a este objetivo. La implementación del CSIRT y el modelo MSPI proporcionan estructuras sólidas que permiten responder eficazmente a incidentes y mantener la seguridad de la información incluso durante interrupciones tecnológicas. Además, la conformación de un equipo de trabajo especializado y la promoción de una cultura de seguridad robusta aseguran que la organización esté preparada para enfrentar y mitigar cualquier interrupción que pueda afectar la operación de los servicios ofrecidos.

Finalmente, el quinto objetivo, "Gestionar eventos e incidentes de seguridad de la información" (OBJ5), se enfoca en fortalecer la capacidad del Ministerio para enfrentar amenazas y ataques informáticos. Las iniciativas INI002, INI003, INI004, INI006 e INI008 son esenciales para este propósito. La implementación del CSIRT sectorial y el modelo MSPI proporcionan herramientas y marcos de trabajo necesarios para detectar, responder y recuperarse de incidentes de seguridad de manera efectiva. La iniciativa INI006, con su enfoque en el cifrado de datos, asegura que incluso en caso de incidentes, la información sensible permanezca protegida. Además, la campaña de cultura de seguridad (INI008) y el establecimiento de un equipo de trabajo especializado (INI004) fortalecen la capacidad organizacional para gestionar y mitigar eventos e incidentes de seguridad de manera proactiva y reactiva.

En síntesis, las iniciativas estratégicas diseñadas por el Ministerio de Salud y Protección Social están cuidadosamente alineadas con sus objetivos estratégicos, asegurando una gestión integral y efectiva de la seguridad de la información. Cada iniciativa aborda aspectos específicos que, en conjunto,

contribuyen a la protección, gestión y resiliencia de los activos de información, garantizando así la sostenibilidad y seguridad de las operaciones del Ministerio.

Código	Iniciativa	OBJ1	OBJ2	OBJ3	OBJ4	OBJ5
INI002	Adquisición de los recursos necesarios para la implementación de los servicios de un CSIRT Sectorial	Sí	Sí	Sí	Sí	Sí
INI003	Implementación del Modelo de Seguridad y Privacidad de la Información-MSPI para todos los procesos de negocio	Sí	Sí	Sí	Sí	Sí
INI004	Establecer un equipo de trabajo para articular y ejecutar las actividades relacionadas con la gestión de seguridad	Sí	Sí	Sí	Sí	Sí
INI006	Implementar un modelo de cifrado de las bases de datos que contienen información de datos personales e información sensible	Sí	Sí	No	No	Sí
INI008	Diseñar una campaña orientada a la cultura de seguridad de la información	Sí	Sí	Sí	Sí	Sí
INI009	Desarrollar una estrategia para la clasificación de activos de información y datos personales	Sí	Sí	No	No	No
INI010	Implementar la gestión de riesgos de seguridad de la información para los activos de información	No	Sí	No	No	No

Ilustración 16 Iniciativas Vs Objetivos Estratégicos SI

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024.

6.3.2. Iniciativas Sectoriales vs. Planes de Política de Seguridad Digital

En este aparte se realiza un análisis sobre el documento *"Catálogo de Iniciativas Sectorial. vs. Planes de la Política de Seguridad Digital V.1.0"*, el cual contiene la matriz de iniciativas presentada para la construcción del presente plan. La matriz se basa en la guía *"Hoja Catálogo"* y contempla las iniciativas alineadas con los Planes de la Política de Seguridad Digital. Las iniciativas están clasificadas según su Prioridad y Duración, proporcionando una visión integral para la toma de decisiones estratégicas que fortalezcan la seguridad digital en el sector, teniendo en cuenta lo siguiente:

1. Alineación Estratégica de los Proyectos
    - **Proyectos de Alta Prioridad:** INI002, INI003, INI008, INI010. Estos proyectos son esenciales para lograr una cobertura integral de la seguridad digital, abarcando desde la gestión de riesgos y la protección de infraestructuras hasta la promoción de una cultura de seguridad.
    - **Proyectos de Media Prioridad:** INI004, INI006, INI009. Aunque su impacto es significativo, no cubren todos los planes estratégicos. Es recomendable considerar su integración en fases futuras o aumentar su alineación estratégica para maximizar su impacto.
2. Gestión del Tiempo en la Implementación de Proyectos
    - **Corto Plazo:** Implementar rápidamente INI004, INI008, INI009, e INI010 permitirá obtener beneficios inmediatos, como la creación de equipos especializados, campañas de concientización y gestión de riesgos.
    - **Mediano Plazo:** No hay iniciativas clasificadas en mediano plazo en la matriz actual, lo que sugiere una posible área de expansión para futuras iniciativas.
    - **Largo Plazo:** INI002, INI003, e INI006 son proyectos complejos que deben abordarse con una estrategia a largo plazo, garantizando sostenibilidad y adaptabilidad.
3. Recursos y Asignación
    - **Recursos Humanos:** La mayoría de las iniciativas requieren gerentes de proyecto, consultores y analistas de seguridad, lo que subraya la necesidad de contar con personal altamente capacitado.
    - **Recursos Tecnológicos:** La implementación de herramientas específicas, como las de cifrado y análisis de vulnerabilidades, es crucial para el éxito de las iniciativas técnicas.
    - **Infraestructura:** Es necesario asegurar que la infraestructura tecnológica soporte adecuadamente las nuevas herramientas y equipos, especialmente para proyectos de CSIRT y cifrado de datos.
4. Fomento de una Cultura de Seguridad Digital
    - **Importancia de INI008:** La campaña de cultura de seguridad es vital para asegurar que todas las iniciativas sean adoptadas y cumplidas por los usuarios finales, aumentando la resiliencia organizacional.

6.3.3. Gobernanza

Para fines de mantenimiento y aseguramiento de la ejecución del Plan Estratégico de Seguridad de la Información (PESI), es fundamental establecer

un marco claro de responsabilidades y liderazgo dentro de la organización. En este sentido, el liderazgo principal estará enmarcado en el Comité Institucional de Gestión y Desempeño (CIGD). Este comité desempeña un papel crucial, debido a que es el organismo encargado de tomar decisiones estratégicas que impactan directamente en el Sistema Integrado de Gestión (SIG), el cual incluye el Sistema de Gestión de Seguridad de la Información (SGSI).

El CIGD no sólo establece las directrices estratégicas, sino que también se asegura de que las iniciativas puedan llevarse a cabo en cuestión de recursos y planeación. En este contexto, su responsabilidad se extiende a priorizar recursos, aprobar estrategias, y monitorear el avance de las actividades relacionadas con el PESI. Este liderazgo garantiza que las decisiones adoptadas en el ámbito del PESI cuenten con el respaldo necesario para su implementación efectiva y sostenible.

Por otro lado, la Oficina de Tecnologías de la Información y la Comunicación (OTIC) desempeña un rol técnico-operativo complementario. Esta oficina es la encargada de realizar la medición del cumplimiento de las estrategias definidas en el PESI, evaluando periódicamente su eficacia. Además, tiene la responsabilidad de identificar, analizar y reportar cualquier desviación detectada en la ejecución del plan. Estas desviaciones podrían surgir debido a factores internos o externos, como cambios en el entorno regulatorio, tecnologías emergentes o nuevas amenazas de seguridad.

La OTIC también tiene la función de proponer acciones correctivas y de mejora, basadas en los resultados de los indicadores y métricas que monitorean la implementación del PESI. Esto permite una gestión proactiva y orientada a la mejora continua, asegurando que las estrategias de seguridad de la información sigan siendo pertinentes y efectivas frente a los cambios desafíos que enfrenta la organización.

6.4. Proyectos

6.4.1. Iniciativas Estratégicas

A continuación, se presenta un conjunto de iniciativas clave diseñadas para impulsar el desarrollo, implementación y seguimiento de proyectos que refuercen la seguridad, eficiencia y sostenibilidad del PESI del sector. Se detallan las características principales de cada iniciativa, incluyendo su propósito, alcance, recursos necesarios y los indicadores de éxito que garantizarán su adecuada ejecución.

ID Iniciativa	INI002
Nombre de la Iniciativa	Adquisición de los recursos necesarios para la implementación de los servicios de un CSIRT Sectorial.
Descripción de la Iniciativa	Implementar un CSIRT que anticipe la materialización de amenazas cibernéticas sobre la infraestructura TI del sector. Además, deberá monitorizar los componentes de las entidades incluidas en su alcance.
Rubro presupuestal	$ 25.429.644.380,00
Plazo	Más de 1 año para su implementación

Tabla 4 Iniciativa Institucional INI002

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

ID Iniciativa	INI008
Nombre de la Iniciativa	Diseñar una campaña orientada a la cultura de seguridad de la información.
Descripción de la Iniciativa	Diseñar e implementar una campaña sectorial que propenda por la apropiación de la cultura de seguridad de la información y protección de datos personales con alcance al Sector Salud.
Rubro presupuestal	$ 582.000.000,00
Plazo	Menos de 6 meses para su implementación

Tabla 5 Iniciativa Institucional INI008

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

ID Iniciativa	INI003
Nombre de la Iniciativa	Implementación del Modelo de Seguridad y Privacidad de la Información-MSPI para todos los procesos de negocio.
Descripción de la Iniciativa	Planificar y desarrollar el MSPI con alcance a todos los procesos de negocio del Sector Salud.
Rubro presupuestal	$ 834.000.000,00
Plazo	Más de 1 año para su implementación

Tabla 6 Iniciativa Institucional INI003

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

ID Iniciativa	INI006
Nombre de la Iniciativa	Implementar un modelo de cifrado de las bases de datos que contienen información de datos personales e información sensible.
Descripción de la Iniciativa	Contratar una herramienta de cifrado que asegure la protección de datos personales con alcance al Sector Salud, considerando el resultado de la identificación y clasificación de activos de información y datos personales.
Rubro presupuestal	$ 1.074.000.000,00
Plazo	Más de 1 año para su implementación

Tabla 7 Iniciativa Institucional INI006

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

ID Iniciativa	INI004
Nombre de la Iniciativa	Establecer un equipo de trabajo para articular y ejecutar las actividades relacionadas con la gestión de seguridad de la información sectorial.
Descripción de la Iniciativa	Conformar un equipo de trabajo especializado para coordinar y llevar a cabo las actividades vinculadas a la gestión de la seguridad de la información a nivel sectorial.
Rubro presupuestal	$ 630.000.000,00
Plazo	Menos de 6 meses para su implementación

Tabla 8 Iniciativa Institucional INI004

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

ID Iniciativa	INI010
Nombre de la Iniciativa	Implementar la gestión de riesgos de seguridad de la información para los activos de información.
Descripción de la Iniciativa	Realizar la gestión de riesgos para los activos de información identificados, que incluya valoración y planes de tratamiento para el Sector Salud.
Rubro presupuestal	$ 624.000.000,00
Plazo	Menos de 6 meses para su implementación

Tabla 9 Iniciativa Institucional INI010

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

ID Iniciativa	INI009
Nombre de la Iniciativa	Desarrollar una estrategia para la clasificación de activos de información y datos personales.
Descripción de la Iniciativa	Fortalecer la gestión de activos mediante la identificación, clasificación y valoración de activos de información y datos personales del Sector Salud.
Rubro presupuestal	$ 329.608.000,00
Plazo	Menos de 6 meses para su implementación

Tabla 10 Iniciativa Institucional INI009

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

6.4.2. Gestión Presupuestal

En el entorno digital actual, la seguridad de la información es crucial para proteger los activos y asegurar la continuidad operativa de las Entidades. El Ministerio de Salud y Protección Social (MSPS) ha identificado una serie de iniciativas estratégicas destinadas a fortalecer la postura de seguridad de la información del sector.

Se identifican siete iniciativas clave para fortalecer la seguridad de la información en el sector. Estas iniciativas varían en su alcance y presupuesto, abarcando desde la formación de equipos especializados hasta la implementación de tecnologías avanzadas para la protección de datos.

6.4.2.1. Iniciativas de Corto Plazo (Prioridad 1)

Estas iniciativas requieren atención inmediata debido a su impacto directo en la gestión y protección de la información sectorial:

1. **Establecer un equipo de trabajo para la gestión de seguridad de la información sectorial (INI004):** Con un gasto estimado de $630.000.000, esta iniciativa es fundamental para coordinar y ejecutar todas las demás actividades relacionadas con la seguridad de la información. Constituye la base organizativa necesaria para una gestión efectiva y centralizada.
2. **Desarrollar una estrategia para la clasificación de activos de información y datos personales (INI009):** Con un costo de $329.608.000, esta iniciativa es crucial para identificar y proteger adecuadamente los activos críticos de información. La clasificación permitirá priorizar recursos y esfuerzos en la protección de información sensible.
3. **Implementar la gestión de riesgos de seguridad de la información para los activos de información (INI010):** Esta iniciativa, con un gasto de $624.000.000, permitirá identificar, evaluar y mitigar riesgos, asegurando la continuidad y seguridad de los procesos del sector. Es esencial para anticipar y responder a posibles amenazas de manera proactiva.

Total de Inversiones de Corto Plazo: $1.583.608.000

6.4.2.2. Iniciativas de Largo Plazo (Prioridad 3)

Estas iniciativas son estratégicas para fortalecer la infraestructura y cultura de seguridad a largo plazo:

1. **Adquisición de los recursos necesarios para la implementación de los servicios de un CSIRT Sectorial (INI002):** Con una inversión significativa de $25.429.644.380, esta iniciativa es crítica para la detección y respuesta ante incidentes de ciberseguridad a nivel sectorial. Un CSIRT robusto permitirá una respuesta coordinada y eficiente ante amenazas emergentes.
2. **Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) para todos los procesos de negocio (INI003):** Con un gasto de $834.000.000, esta iniciativa establece un marco integral de seguridad y privacidad que abarca todos los procesos de negocio, asegurando una protección coherente y estandarizada de la información.
3. **Implementar un modelo de cifrado de las bases de datos que contienen información de datos personales e información sensible (INI006):** Con un presupuesto de $1.074.000.000, esta iniciativa

garantiza la protección de datos sensibles mediante tecnologías de cifrado avanzadas, reduciendo el riesgo de accesos no autorizados y brechas de seguridad.

4. **Diseñar una campaña orientada a la cultura de seguridad de la información (INI008):** Con un costo de $582.000.000, esta campaña fomentará una cultura organizacional orientada a la seguridad, aumentando la concienciación y reduciendo riesgos derivados de errores humanos.

Total de Inversiones de Largo Plazo: $27.919.644.380

En este sentido, se deben tener en cuenta las siguientes consideraciones:

1. **Priorización de Iniciativas de Corto Plazo:** Dada su alta prioridad y menor costo relativo, se recomienda iniciar inmediatamente con las iniciativas INI004, INI009 e INI010. Estas establecerán las bases necesarias para una gestión efectiva de la seguridad de la información, facilitando la implementación de iniciativas posteriores.
2. **Planificación Financiera para Iniciativas de Largo Plazo:** La implementación del CSIRT Sectorial (INI002) representa una inversión significativa. Es esencial desarrollar un plan financiero detallado que contemple la financiación gradual, posiblemente en fases, para asegurar la viabilidad presupuestaria y evitar sobrecargas financieras.
3. **Sinergias entre Iniciativas:** Las iniciativas de largo plazo pueden beneficiarse de la infraestructura y cultura establecida por las de corto plazo. Por ejemplo, la campaña de cultura de seguridad (INI008) potenciará la efectividad de la gestión de riesgos (INI010), creando un entorno más resiliente ante amenazas.
4. **Evaluación Continua y Ajustes:** Es fundamental establecer mecanismos de monitoreo y evaluación para todas las iniciativas, permitiendo ajustes oportunos en función de los avances y cambios en el entorno de amenazas. Esto garantizará que el plan estratégico permanezca relevante y efectivo a lo largo del tiempo.
5. **Capacitación y Desarrollo:** Invertir en la capacitación continua del equipo de seguridad (INI004) es crucial para asegurar que estén preparados para manejar las complejidades de las iniciativas futuras, especialmente la implementación del CSIRT y la gestión de riesgos avanzados.

El plan estratégico presentado abarca iniciativas esenciales para fortalecer la seguridad de la información en el Sector Salud. Al priorizar las acciones de corto plazo y planificar adecuadamente las inversiones a largo plazo, se asegura una implementación efectiva y sostenible. La asignación eficiente de recursos y la coordinación entre las iniciativas serán clave para el éxito global del plan,

garantizando una protección robusta y resiliente frente a las amenazas cibernéticas actuales y futuras.

6.4.3. Hoja de Ruta

La hoja de ruta del PESI sectorial establece una planificación estratégica detallada para el fortalecimiento de la seguridad de la información en el ámbito sectorial de salud. Distribuida desde 2025 hasta 2028, tal como se establece en el documento *MSPS_Hoja de Ruta PESI_Sectorial,* esta herramienta destaca los proyectos clave, como la implementación de un CSIRT sectorial, el establecimiento de modelos de seguridad y privacidad, y la gestión de riesgos. Cada iniciativa está diseñada para garantizar la protección de la información sensible, promoviendo una cultura de ciberseguridad y asegurando la continuidad operativa a través de inversiones planificadas y ejecución coordinada.

HOJA DE RUTA DE PESI SECTORIAL

Proyecto: CONTRATAR LA ELABORACIÓN Y SOCIALIZACIÓN DE LOS PLANES DE TRANSFORMACIÓN DIGITAL EN LOS COMPONENTES DE ARQUITECTURA EMPRESARIAL, PTD Y PETI, GOBIERNO Y CALIDAD DE DATOS, PESI Y BCP Y FORTALECIMIENTO Y AUTOMATIZACIÓN DE TRAMITES, PARA EL MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL.

Proyectos	2025				2026				2027				2028			
	TRIMESTRE 1	TRIMESTRE 2	TRIMESTRE 3	TRIMESTRE 4	TRIMESTRE 1	TRIMESTRE 2	TRIMESTRE 3	TRIMESTRE 4	TRIMESTRE 1	TRIMESTRE 2	TRIMESTRE 3	TRIMESTRE 4	TRIMESTRE 1	TRIMESTRE 2	TRIMESTRE 3	TRIMESTRE 4
	01 02 03	04 05 06	07 08 09	10 11 12	01 02 03	04 05 06	07 08 09	10 11 12	01 02 03	04 05 06	07 08 09	10 11 12	01 02 03	04 05 06	07 08 09	10 11 12
PRY002 - Adquisición de los recursos necesarios para la implementación de los servicios de un CSIRT Sectorial.																
PRY003 - Implementación del Modelo de Seguridad y Privacidad de la Información-MSPI para todos los procesos de negocio.																
PRY004 - Establecer un equipo de trabajo para articular y ejecutar las actividades relacionadas con la gestión de seguridad de la información sectorial.																
PRY006 - Implementar un modelo de cifrado de las bases de datos que contienen información de datos personales e información sensible.																
PRY008 - Diseñar una campaña orientada a la cultura de seguridad de la información.																
PRY009 - Desarrollar una estrategia para la clasificación de activos de información y datos personales.																
PRY010 - Implementar la gestión de riesgos de seguridad de la información para los activos de información.																
	$ 8.388.019.095,00				$ 7.893.411.095,00				$ 6.894.411.095,00				$ 6.357.411.095,00			
	Proyectos en curso		5		Proyectos en curso		4		Proyectos en curso		2		Proyectos en curso		1	
	TOTAL ESTIMADO EN PROYECTOS DE INVERSIÓN												$ 29.533.252.380,00			

Ilustración 17 Hoja de Ruta PESI_Sectorial

Fuente elaboración propia UT MYQ ALINATECH PETI 2024 MSPS_Hoja de Ruta PESI_Sectorial

6.5. Medición E Indicadores

La medición del presente plan, se enfoca en la evaluación del *"Tablero de Indicadores PESI SECTORIAL"*, diseñado para monitorear y medir el desempeño de las iniciativas del Plan Estratégico de Seguridad de la Información (PESI) SECTORIAL. El tablero incluye una serie de indicadores que permiten evaluar la

ejecución, eficacia y eficiencia de los proyectos, facilitando la toma de decisiones estratégicas y la optimización de recursos del sector salud.

1. Alineación Estratégica de los Indicadores

- Cobertura Integral: Todos los indicadores están alineados con los objetivos estratégicos del PESI, enfocándose en aspectos críticos como la ejecución de proyectos, gestión presupuestal, control de costes, gestión de riesgos y finalización de proyectos. Esta alineación asegura que se monitoreen las áreas clave para el éxito del plan estratégico.

- Tipo de Indicadores: La mayoría son indicadores de proyectos, lo que refleja una fuerte orientación hacia la gestión y ejecución de iniciativas. Este enfoque permite evaluar tanto la planificación como la implementación efectiva de los proyectos dentro del PESI.

2. Frecuencia y Gestión de Datos

- Frecuencia de Medición: Los indicadores se miden principalmente de manera semestral, con uno anual y otro trimestral. Esta periodicidad es adecuada para un seguimiento constante y oportuno, permitiendo identificar y abordar desviaciones a tiempo.

- Origen de los Datos: Los datos provienen de fuentes internas como el tablero de control de proyectos, desembolsos realizados, matriz de riesgos y actas de cierre de proyectos. Esto garantiza la fiabilidad y consistencia de la información utilizada para los cálculos de los indicadores.

3. Responsables y Asignación de Recursos

- Centralización de la Responsabilidad: Todos los indicadores están bajo la responsabilidad de la OTIC (Oficina de Tecnología de la Información y Comunicaciones). Esta centralización facilita una gestión coherente y uniforme de los datos, asegurando una interpretación consistente de los resultados.

- Recursos Asignados: La asignación de responsables claros para cada indicador asegura una rendición de cuentas efectiva y facilita la identificación de áreas que requieren atención o mejora.

4. Metas y Rangos de Desempeño

- Metas Claras: Todos los indicadores tienen una meta establecida del 100%, lo que refleja un objetivo de máxima eficiencia y cumplimiento en la ejecución de los proyectos del PESI.

- Rangos de Desempeño: La categorización en rangos (>=95%, Entre 94% y 71%, <=70%) permite una rápida evaluación del desempeño y facilita la identificación de áreas que necesitan intervención inmediata o ajustes estratégicos.

5. Eficacia y Eficiencia en la Gestión de Proyectos

- Eficacia en la Gestión del Riesgo: El indicador IND.PESI.SECT.005 es crucial para medir la eficacia de los controles de riesgo implementados, asegurando que los riesgos identificados sean gestionados adecuadamente y minimizando la materialización de estos.

- Control Presupuestal: Indicadores como IND.PESI.SECT.003 y IND.PESI.SECT.004 permiten evaluar la eficiencia en la gestión presupuestal y el control de costes, asegurando que los proyectos se ejecuten dentro de los fondos asignados.

6. Monitoreo y Evaluación Continua

- Seguimiento Regular: La periodicidad de los indicadores permite un seguimiento continuo y facilita la identificación temprana de desviaciones, permitiendo la implementación de acciones correctivas a tiempo.

- Evaluación Integral: La combinación de indicadores de ejecución, presupuestales y de riesgos proporciona una visión integral del desempeño del PESI, permitiendo una gestión más informada y estratégica.

6.6. Uso y Apropiación

Es importante generar acciones que lleven al uso y apropiación del PESI en el Ministerio de Salud y Protección Social, como en las entidades adscritas al Sector Salud, estas acciones determinan que el plan no de quede formulado en un documento y se ejecute de manera particularizada en el área responsable, su efectividad depende de que en el día a día tanto los usuarios técnicos como los usuarios funcionales lo gestionen y lo adopten de manera natural, teniendo en cuenta los lineamientos del MSPS y la Resolución 500 del 2021, se plantean las siguientes acciones:

1. **Sensibilización:** Se busca que los usuarios funcionales tomen consciencia de la importancia que tiene la seguridad de la información para:

- La Entidad, tanto a nivel organizacional por salvaguardar uno de los activos más importantes para la continuidad y sostenibilidad operativa, como la reputación y credibilidad de la misma.

- Individual, como su compromiso ético y cumplimiento normativo de ser responsable con la información que maneja en su día a día, y que para ello debe evidenciar unos comportamientos como:

    - Cumplir con las políticas y normas de seguridad de la información.
    - Facilitar el acceso a la información pública, completa, veraz, oportuna y comprensible a través de los medios destinados para ello.
    - Ser cuidadoso con la información a su cargo, y con su gestión.
    - Tener la información segura.
    - Reportar de inmediato un correo electrónico sospechoso que parece ser phishing.
    - Bloquear el equipo al retirarse de su lugar de trabajo.
    - No abrir enlaces desconocidos.
    - Llamar directamente al Oficina de TIC para confirmar una solicitud de datos financieros antes de responder.
    - No utilizar las credenciales de otro compañero para acceder a sistemas.
    -

La Sensibilización se puede llevar a cabo a través de mensajes claves que le permita a los usuarios funcionales entender los beneficios que tiene el Plan Estratégico de la Seguridad de la información – PESI, tanto para la entidad y para ellos de manera particular; también a través de reuniones por áreas que involucre al líder de la misma sobre los posibles riesgos asociados a la seguridad de la información y finalmente diferentes piezas de comunicación por diferentes canales, para posicionar la seguridad de la información en los usuarios funcionales.

2. **Capacitación:** facilitar escenarios de aprendizaje a

- ***Usuarios técnicos*** en temas como: Procedimiento para informar posible phishing, Gestión de Riesgos en la Seguridad de la Información, Control de Acceso y Autenticación, Protección contra Amenazas Cibernéticas, Seguridad en la Gestión de Datos, Respuestas ante Incidentes de Seguridad, Concientización sobre Ingeniería Social y Phishing, Protección de Infraestructuras y Sistemas Crítico, Evaluación, Auditoría y Mejora Continua, Seguridad en el Desarrollo de Software, Capacitación Específica por Rol y Pruebas de Seguridad y Simulación

- ***Usuarios funcionales*** como: Políticas, Normativas y Protocolos de Seguridad (Ley 1581 de 2012, Resolución 500 de 2021 del MSPS, entre

otras), Identificación de amenazas de seguridad de información, Procedimiento para informar posible phishing, Como identificar un Phishing.

- Realizar simulacros de incidentes de seguridad de la información o jornadas trimestrales pedagógicas puesto a puesto, para fortalecer temas puntuales de seguridad, por ejemplo: Pregúntale al colaborador cuál es su responsabilidad con la seguridad de la información, escuche y refuerce, cual es el procedimiento para reportar un posible phishing, a quien reporta, etc.…

- Realizar Mentorías. Defina un grupo de guardianes de la seguridad, uno por área, quien será la extensión del área de seguridad de la información al interior de las oficinas (su voz y sus oídos).

3. **Comunicación:** Mensajes claves por diferentes canales con una periodicidad inicial mensual y posterior trimestral, estos pueden ser en el boletín "El Saludable", correos electrónicos, cartelera digital, banners en la intranet, así mismo al interior de la intranet un micrositio de Seguridad de la información, que permita un SOS (Botón de alerta).

4. **Monitoreo y Seguimiento:** Con auditorías internas frente al PESI, definición de indicadores como el cumplimiento de las políticas internas de seguridad de información o reducción de incidentes y finalmente encuestas para identificar la cultura de la seguridad de la información.

Con estas acciones se espera que, en la entidad haya una mayor apropiación de la seguridad de la información a través de un cumplimiento normativo, unos comportamientos asociados a proteger y dar buen uso a la información y finalmente una reducción de incidentes.

7. CONCLUSIONES

- Las iniciativas de alta prioridad garantizan una cobertura integral de la seguridad digital, abarcando aspectos críticos como la gestión de riesgos, protección de infraestructuras y promoción de una cultura de seguridad.
- Los proyectos clasificados en corto plazo proporcionan beneficios inmediatos y establecen una base sólida para iniciativas más complejas a mediano y largo plazo.
- La implementación efectiva de las iniciativas requiere una asignación adecuada de recursos humanos y tecnológicos especializados, subrayando la importancia de contar con personal capacitado y herramientas avanzadas.
- Una estructura de gobernanza robusta es esencial para coordinar todas las iniciativas, evitar redundancias y optimizar el uso de recursos, asegurando la eficiencia y efectividad del plan estratégico.
- Promover una cultura de seguridad digital es crucial para la adopción y el cumplimiento de las medidas de seguridad, incrementando la resiliencia organizacional y la confianza de los usuarios en los servicios digitales.
- Los proyectos de largo plazo requieren una estrategia sostenida que garantice su adaptabilidad frente a futuros desafíos tecnológicos y cambios en el entorno de amenazas.
- Es fundamental realizar evaluaciones periódicas para medir el progreso de las iniciativas, permitiendo ajustes oportunos y asegurando la relevancia continua del plan estratégico.
- Los indicadores seleccionados cubren aspectos críticos de la ejecución de proyectos, incluyendo el cumplimiento de plazos, presupuestos y gestión de riesgos. Esto garantiza una visión completa del desempeño del PESI y facilita la identificación de áreas que requieren mejoras.
- La frecuencia semestral y anual de los indicadores permite un seguimiento constante y oportuno del progreso de los proyectos, facilitando la detección temprana de desviaciones y la implementación de acciones correctivas.
- La asignación de la responsabilidad a la OTIC asegura una gestión centralizada y coherente de los datos, mejorando la precisión y confiabilidad de los indicadores.

- La definición de metas claras y rangos de desempeño facilita la evaluación objetiva del progreso y ayuda a identificar áreas que requieren atención especial.

- Los indicadores están diseñados para medir tanto la eficiencia en la ejecución de proyectos como la eficacia en la gestión de riesgos, contribuyendo a la optimización de recursos y al logro de los objetivos estratégicos del MSPS.

- El indicador de eficacia en la gestión de riesgos asegura que los controles implementados son efectivos, reduciendo la probabilidad de materialización de riesgos y mejorando la resiliencia del PESI.

8. BIBLIOGRAFÍA

Mintic. (2021). *Documento Maestro, Seguridad y Privacidad de la Información.* Recuperado de https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-162621_Modelo_de_Seguridad_y_Privacidad__MSPI.pdf

Mintic. (2021). *Anexo 1, Seguridad y Privacidad de la Información*. Recuperado de https://www.mintic.gov.co/portal/715/articles-160599_recurso_2.pdf

MinSalud. (2018). *Plataforma estratégica 2018-2021*. Entregado como insumo para el proyecto.

MinSalud. (2024). *Contexto Estratégico de Seguridad de la Información*. Entregado como insumo para el proyecto.

MinSalud. (2023). *Manual del Sistema de Gestión de Seguridad en la Información.* Entregado como insumo para el proyecto.

MinSalud. (2024). *Informe Auditoría Interna, Ciclo I-2024.* Entregado como insumo para el proyecto.

INS. (2023). *Informe de Diagnóstico Tecnologías de la Información*. Entregado como insumo para el proyecto.

INS. (2024). Plan Estratégico de Seguridad de la Información. Entregado como insumo para el proyecto.

ADRES. (2023). *Plan Estratégico de Tecnologías de la Información 2023-2026.* Entregado como insumo para el proyecto.

FONFEROCARRILES. (2023). *Formato*

9. DOCUMENTOS REFERENCIA

MSPS_Contexto Estratégico Seguridad Información

MSPS_Análisis del Entorno del MSPS y el Sector Salud

MSPS_ Análisis_DOFA_PESTEL

MSPS_ Diagnóstico de Seguridad Digital Institucional y Sectorial

MSPS_Análisis y Comprensión de los Hallazgos y Oportunidades de Mejora

MSPS_Ficha y Catálogo de Iniciativas de Inversión_Sectorial

MSPS_Catálogo de Iniciativas Sectorial. vs. Planes de la Política de Seguridad Digital

MSPS_Acta constitución proyecto_INI003_Sectorial

MSPS_Acta constitución proyecto_INI004_Sectorial

MSPS_Acta constitución proyecto_INI006_Sectorial

MSPS_Acta Constitución Proyecto_INI008_Sectorial

MSPS_Acta constitución proyecto_INI009_Sectorial

MSPS_Acta constitución proyecto_INI010_Sectorial

MSPS_Ficha y Catálogo de Gastos sobre la Operación de SI_Sectorial

MSPS_Hoja de Ruta PESI_Sectorial

MSPS_Tablero de Indicadores PESI

MSPS_Estrategia de Comunicación PESI -MSPS y Sectorial

MSPS_Plan de Transferencia de Conocimiento PESI Institucional y Sectorial

10. GLOSARIO

Termino	Definición
Activo de Información	Conjunto de datos, sistemas, infraestructura, personas y procesos que permiten gestionar y proteger información valiosa para una organización.
Análisis DOFA	Herramienta de diagnóstico estratégico que permite identificar las Debilidades, Oportunidades, Fortalezas y Amenazas en un contexto específico.
BCP	Business Continuity Plan - Plan de Continuidad del Negocio. Proceso para asegurar que las operaciones críticas continúen durante y después de una interrupción.
Ciclo PHVA	Metodología de mejora continua que comprende las etapas de Planear, Hacer, Verificar y Actuar, aplicada en la gestión de sistemas como el SGSI.
Confidencialidad	Principio de seguridad de la información que asegura que los datos solo sean accesibles a personas o sistemas autorizados.
Continuidad del Negocio	Capacidad de una organización para continuar sus operaciones críticas durante y después de un evento disruptivo.
Disponibilidad	Garantía de que la información y los sistemas están accesibles para los usuarios autorizados cuando los necesiten.
DOFA	Debilidades, Oportunidades, Fortalezas y Amenazas. Herramienta analítica utilizada para evaluar la situación actual de una organización.
DRP	Disaster Recovery Plan - Plan de Recuperación ante Desastres. Estrategia para restaurar sistemas de información y datos en caso de incidentes graves.
Gestión de Incidentes de Seguridad	Proceso de identificación, análisis y respuesta a eventos que comprometen la seguridad de la información.
Gestión de Riesgos	Evaluación y tratamiento de amenazas potenciales que puedan afectar la confidencialidad, integridad o disponibilidad de los activos de información.
Gobernanza de Seguridad de la Información	Proceso mediante el cual se gestionan y controlan las políticas, roles y responsabilidades relacionadas con la protección de la información.
Integridad	Principio que garantiza que los datos no han sido alterados de manera no autorizada y que son confiables.
ISO/IEC 27001	Norma internacional sobre gestión de seguridad de la información.
MAE	Modelo de Arquitectura Empresarial. Marco metodológico para alinear procesos y tecnologías con los objetivos estratégicos de una organización.
MinTIC	Ministerio de Tecnologías de la Información y las Comunicaciones. Entidad gubernamental de Colombia

Termino	Definición
	encargada de las políticas de transformación digital y seguridad de la información.
Modelo de Seguridad y Privacidad de la Información (MSPI)	Estructura que integra políticas, procedimientos y controles para proteger los activos de información y garantizar la privacidad de los datos personales.
MSPI	Modelo de Seguridad y Privacidad de la Información. Enfoque sistemático para gestionar riesgos de seguridad digital en el sector público.
MSPS	Ministerio de Salud y Protección Social. Entidad gubernamental colombiana responsable de las políticas de salud pública.
NTC	Norma Técnica Colombiana. Estándares nacionales aplicados en diversos sectores.
OTIC	Oficina de Tecnologías de la Información y las Comunicaciones. Área encargada de la infraestructura tecnológica y sistemas de información.
PESI	Plan Estratégico de Seguridad de la Información. Documento estratégico para garantizar la protección de los activos de información.
PGD	Política de Gobierno Digital. Lineamientos para la transformación digital en la administración pública.
PHVA	Planear, Hacer, Verificar y Actuar. Ciclo de mejora continua aplicado en la gestión de la seguridad de la información.
PIC	Plan Institucional de Capacitación. Estrategia para formar y sensibilizar al personal en diversas competencias.
Plan de Recuperación ante Desastres (DRP)	Conjunto de estrategias y procedimientos destinados a restaurar sistemas y datos críticos tras un incidente grave.
Política de Seguridad de la Información	Documento que define las directrices, normas y procedimientos para proteger los activos de información de una organización.
SABSA	Sherwood Applied Business Security Architecture. Marco de referencia para desarrollar arquitecturas de seguridad basadas en riesgos.
SGSI	Sistema de Gestión de Seguridad de la Información. Conjunto de políticas, procedimientos y controles para gestionar la seguridad de los datos.
SIC	Superintendencia de Industria y Comercio. Autoridad colombiana responsable de la protección de datos personales.
SIG	Sistema Integrado de Gestión. Plataforma que agrupa diversas normas y procedimientos organizacionales.
Sistema de Gestión de Seguridad de la Información (SGSI)	Conjunto de políticas y controles integrados para proteger y gestionar la seguridad de la información de manera sistemática.

Termino	Definición
TI	Tecnologías de la Información. Conjunto de recursos tecnológicos utilizados para la gestión de la información.
TIC	Tecnologías de la Información y las Comunicaciones. Tecnologías que integran telecomunicaciones y sistemas de información.
Transformación Digital	Proceso de integración de tecnologías digitales en todas las áreas de una organización, mejorando su eficiencia y capacidad de adaptación.

Tabla 11 Nombre Glosario
Fuente: elaboración propia UT MYQ ALINATECH PETI 2024