Plan Estratégico de Seguridad de la Información Institucional 2024-2028

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 con los insumos obtenidos.	Documento con el Plan Estratégico de Seguridad de la información Institucional.

1. INTRODUCCIÓN

Considerando los riesgos principales a nivel mundial en cuanto a la seguridad de la información, la protección de esta es una prioridad fundamental para las organizaciones en general, pero más aún para las entidades gubernamentales y en particular para aquellas que manejan una gran cantidad de información de los ciudadanos, como lo es el sector salud en Colombia.

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.

La transformación digital apoya el desarrollo del sector salud, aunque de manera concomitante podría incrementarse la superficie de exposición de riesgos que afecten los principios de integridad, confidencialidad y disponibilidad de la información tanto del Ministerio de Salud y Protección Social (MSPS), como del sector en general. 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 el Ministerio de Salud y Protección Social (MSPS), dentro de los cuales se incluye el Plan Estratégico de Seguridad Información (PESI), el cual es parte integral de la estrategia institucional del Ministerio 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.

Este plan es un instrumento esencial para fortalecer la seguridad de la información en el ecosistema de salud colombiano y se alinea con las mejores prácticas internacionales y normativas vigentes locales, lo que garantiza que el sector salud colombiano opere en una forma que mejora la calidad de vida de todos los ciudadanos. Este documento toma como insumo la plantilla desarrollada por el MinTIC para la elaboración del Plan de Seguridad y Privacidad de la Información o (PESI), que permite cumplir con los requisitos del establecimiento de la estrategia de seguridad digital de acuerdo con lo establecido en el artículo cinco de la resolución 500 de 2021.

Se busca, por otro lado, presentar en este documento las actividades realizadas con el objetivo de crear el documento del PESI Institucional. El primer hito corresponde el estado actual del dominio de seguridad de la información institucional mediante la elaboración de un diagnóstico que sirve como insumo para la planeación del PESI Institucional. El segundo Hito corresponde a la estructuración de iniciativas y proyectos que en un determinado tiempo deben contribuir a la disminución de los riesgos identificados en el Hito número uno.

Finalmente, este documento comprende las fases propuestas para la construcción del PESI propuestas por el MSPS que son en su respectivo orden: comprender, analizar, construir y presentar.

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 institucional para el período 2024-2028, alineada con los necesidades institucionales 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 de la Entidad como cabeza de sector.

2.2. Objetivos Específicos

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

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

3. ALCANCE

El alcance de este documento está orientado en definir conceptualmente el diagnóstico de situación actual y las iniciativas del PESI Institucional. Por otra parte, aplica a todos los procesos y activos de información del Ministerio de Salud y Protección Social. 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 de la Entidad.

4. MARCOS METODOLÓGICOS

4.1. Marco Metodológico General del Proyecto

Con el propósito de presentar los marcos metodológicos utilizados para la elaboración del PESI Institucional, a continuación, se presenta una breve descripción de las fases para la construcción del PESI desde la perspectiva general del proyecto:

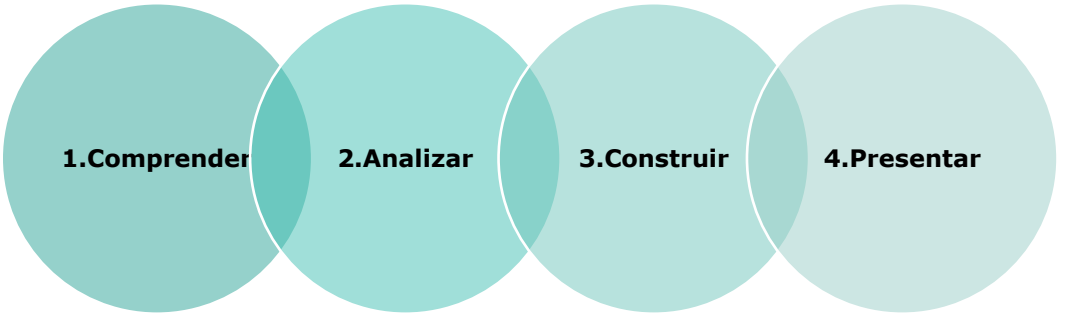

Ilustración 1 Fases del proyecto PESI

Fuente: MSPS.

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

Fase Analizar: en esta fase se realiza el estudio de la situación actual 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 Institucional 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 el MSPS cuenta 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 la Entidad.

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 sus 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) y las fases de Conocer, Planear, Ejecutar y Medir:

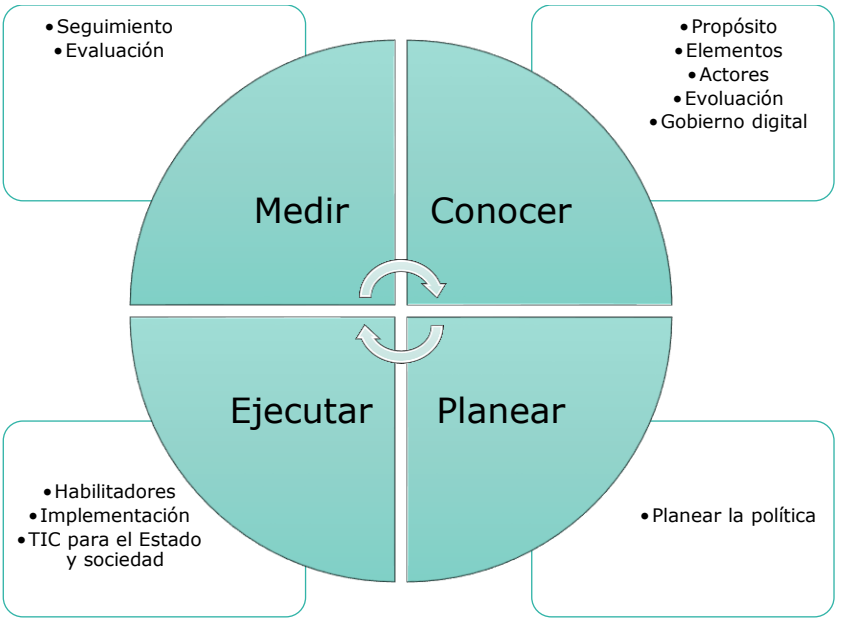

Ilustración 2 Fases de la Política de Gobierno Digital

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. El MSPS debe 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, más los lineamientos recibidos por parte de la normatividad vigente a nivel nacional o internacional, para implementar una serie de medidas de proyección alineadas con los objetivos estratégicos de la Entidad.

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.

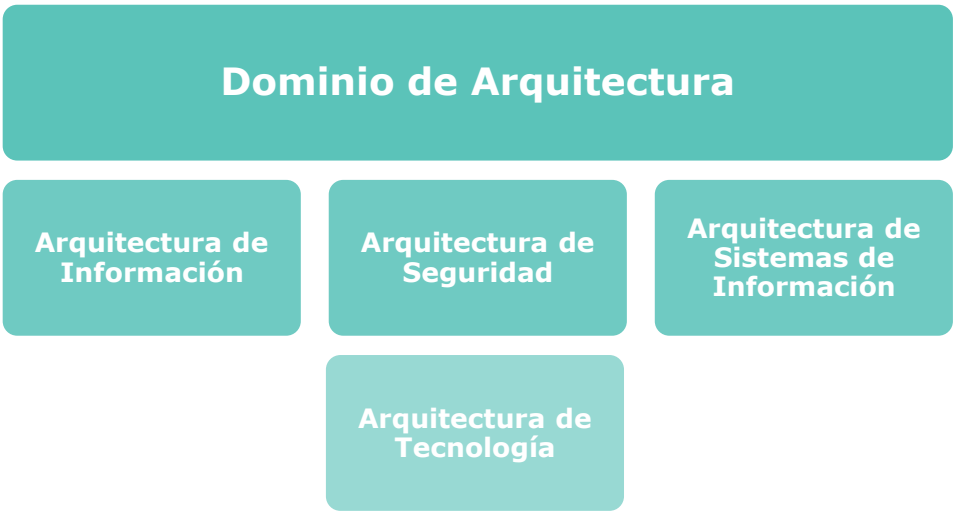

Ilustración 3 Modelo MAE de arquitectura empresarial.

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.

Por otra parte, 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: Diagnóstico, Planificación, Operación, Evaluación de desempeño, Mejoramiento continuo:

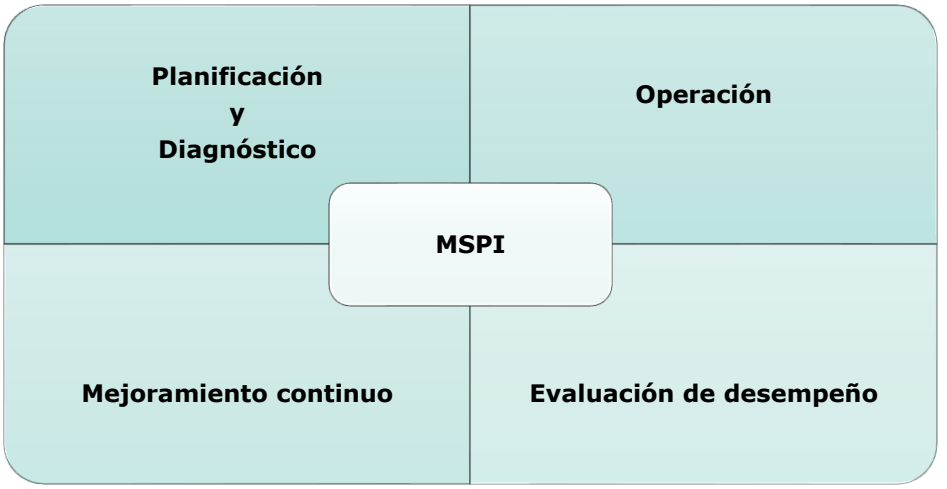

Ilustración 4 Modelo de Seguridad y Privacidad de la Información

Fuente: MSPI, MinTIC.

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

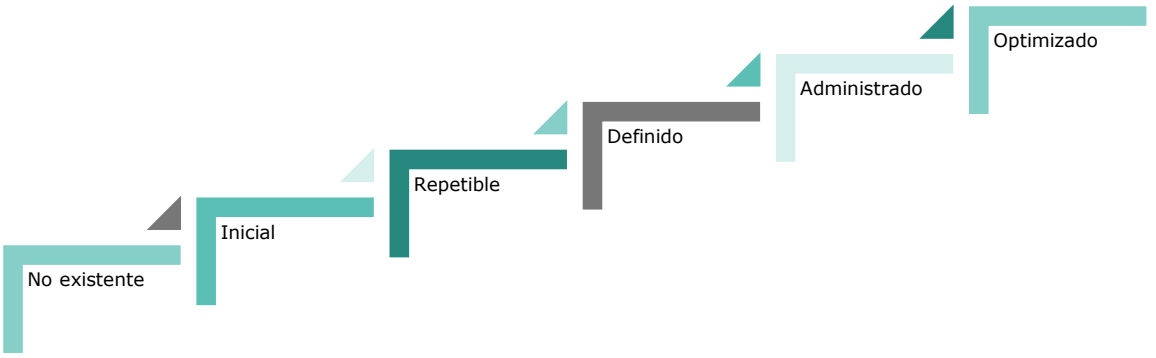

Ilustración 5 Niveles de madurez según Gartner.

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.

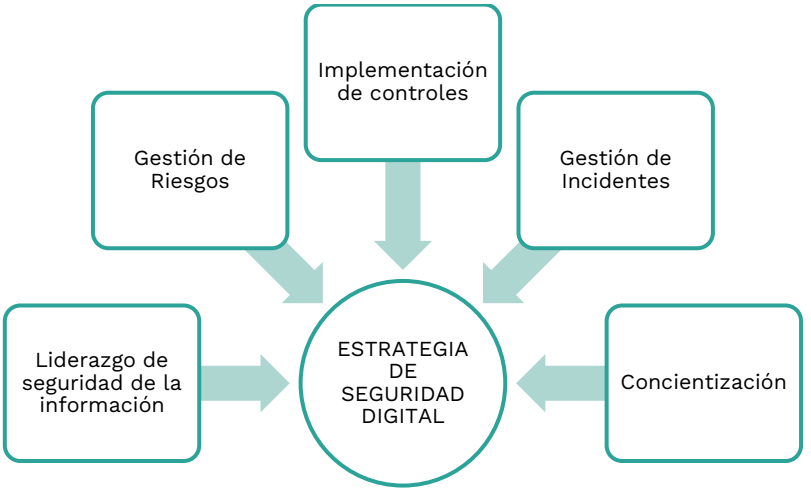

Ilustración 6 Metodología o plantilla para el PESI.

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 Modelo de Seguridad y Privacidad de la Información (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 la Entidad.

Gestión de incidentes: garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad.

4.7. Metodología DOFA y PESTEL

En la construcción del PESI para el MSPS se requiere analizar las debilidades, fortalezas, oportunidad y amenazas del área de seguridad de la información de la Oficina de Tecnologías de la Información y las Comunicaciones (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 la Entidad.

La metodología DOFA permite identificar las condiciones internas (fortalezas y debilidades) de la organización 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.

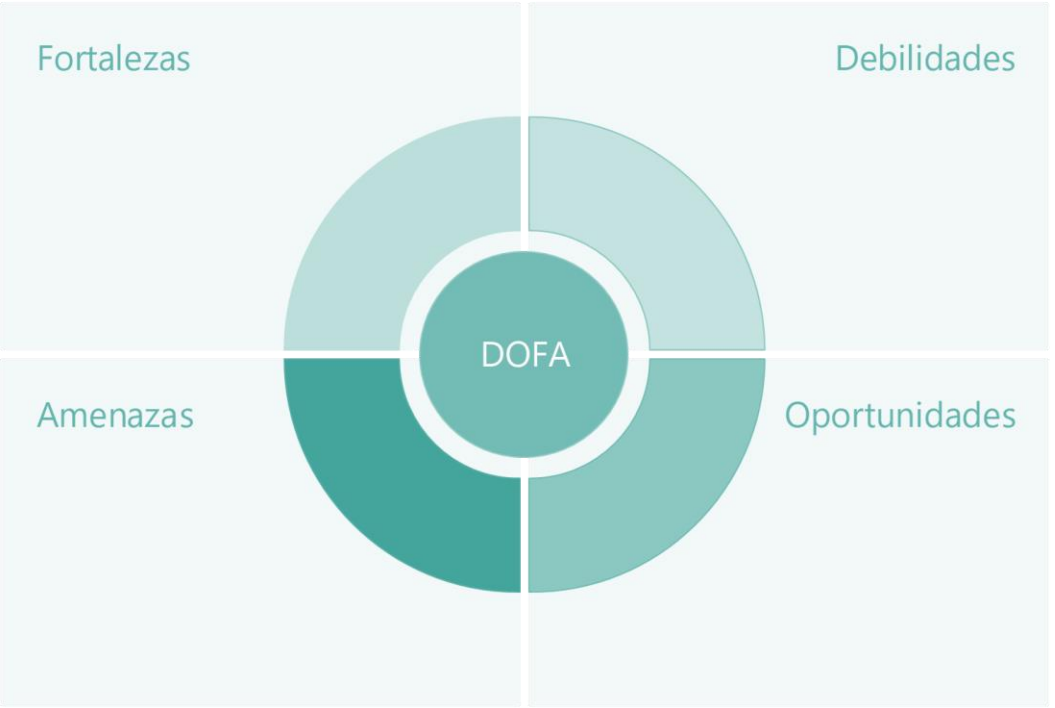

Ilustración 7 Cuadrantes de la matriz DOFA.

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 INSTITUCIONAL 2024-2028", 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:

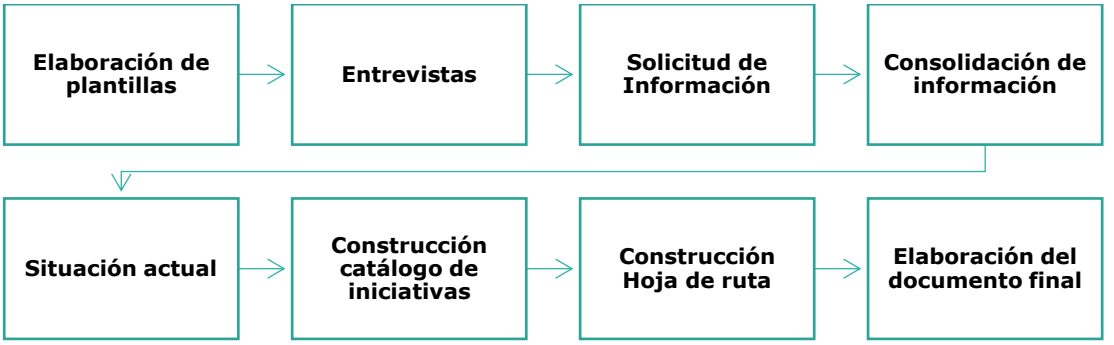

Ilustración 8 Metodología para elaboración del entregable

Fuente: Propia.

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 del MSPS.

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 del MSPS.

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 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 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 INSTITUCIONAL

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 MSP 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 MSPS

A continuación, se presenta el contexto estratégico del MSPS:

En la revisión del Eje Estratégico de Implementación de Controles, no se evidencia con certeza que los controles de seguridad informática implementados mitiguen efectivamente los riesgos misionales del MSPS. Esto se debe a que la gestión de activos y riesgos de los procesos misionales no se realiza con base en un enfoque integral de arquitectura empresarial. No obstante, se reconoce que la entidad cuenta con controles que mitigan riesgos que corresponden a otros procesos del Ministerio.

La revisión del Eje Estratégico de Gestión de Riesgos del MSPS permite observar que el MSPI no tiene alcance a los procesos misionales, que son los que procesan la información más sensible del Ministerio; esta situación genera incertidumbre frente eventos que no se están controlando.

En la revisión del Eje Estratégico de Gestión de Incidentes es evidente que el Ministerio cuenta con procedimientos formales para la atención de eventos e incidentes, además, el MSPS tiene una infraestructura robusta de cacería de amenazas y control de phishing con el fabricante Fortinet, pero no se lleva un registro cuidadoso de los eventos e incidentes gestionados, perdiendo relevancia las lecciones aprendidas.

La revisión del Eje Estratégico de Liderazgo permite identificar que el MSPS cuenta con el apoyo de la Alta Dirección representada en el Comité Institucional de Gestión y Desempeño, lo que ha permitido elevar al MSPS al nivel de certificación ISO/IEC 27001, no obstante, el liderazgo de equipo de seguridad de la información se ve limitado por el grupo de soporte informático adscrito a la Secretaría General, quienes son los responsables de gestionar los controles tecnológicos.

En la revisión del Eje Estratégico de Concientización se observa que hay significativos avances capacitación, formación y educación. Sin embargo, aún muchos colaboradores, usuarios finales y contratistas tienen un nivel bajo de conocimiento sobre la ciberseguridad.

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 Resolución 500 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

Además, para la elaboración de este diagnóstico de la situación actual del MSPS se analizaron los siguientes componentes del MSPI:

- 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

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. Documentos del MSPI del MSPS

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

Roles y Responsabilidades (60%): las funciones del Oficial de Seguridad de la Información están en cabeza del jefe OTIC, además, en el Manual del SGSI están definidos los siguientes segmentos de responsabilidades: estratégico, táctico, operativo, participantes y/o población.

Existen dos grupos que ejecutan actividades relacionadas con seguridad digital: a. Gobierno del MSPI en OTIC y b. Soporte Informático en Secretaría General.

Estos roles y responsabilidades están separados, por lo que no hay una gestión efectiva del MSPI en la articulación de políticas con la aplicación de controles.

Políticas de seguridad de la información (60%): existe una alta alineación a la Guía No. 2 Elaboración de la Política General de Seguridad y Privacidad de la Información del MSPI, además el MSPS tiene cumplimiento de los requisitos establecidos en el numeral 5.2 de la ISO 27001:2022. El conjunto de políticas específicas cubre los requisitos mínimos establecidos por el MSPI y la NTC ISO/IEC 27001:2022, pero no fueron revisados y actualizados en 2024.

Procesos y procedimientos de seguridad de la información (60%): en general, el MSPS 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 (40%): la entidad cuenta con documento de política de clasificación de información, guía para el levantamiento y valoración de activos, y formato (matriz) de inventario de activos, no obstante, solamente se registra la matriz de activos para ocho procesos del MSPS.

Metodología de gestión de riesgos, matriz de riesgos, plan de tratamiento de riesgos, plan de tratamiento de riegos y controles de seguridad (40%): la entidad cuenta con un procedimiento de gestión de riesgos, aplicado en el instrumento de matriz de riesgos y siguiendo la metodología con la asignación de controles. Pero, no todos los procesos misionales cuentan con la evaluación y gestión de riesgos.

Gestión de la cultura de seguridad digital (60%): el MSPS Se cuenta con un Plan Institucional de Capacitación PIC 2024 en el que se abordan generalidades de seguridad digital, así como temas especializados; no obstante, no se identifica un plan de sensibilización y toma de conciencia que involucre a todos los contratistas. Cabe destacar que el PIC 2024 se gestiona con indicadores de desempeño.

Auditoría y revisión del MSPI (80%): para la vigencia del periodo el MSPS cumplió con el ciclo de auditoría interna y auditoría de seguimiento.

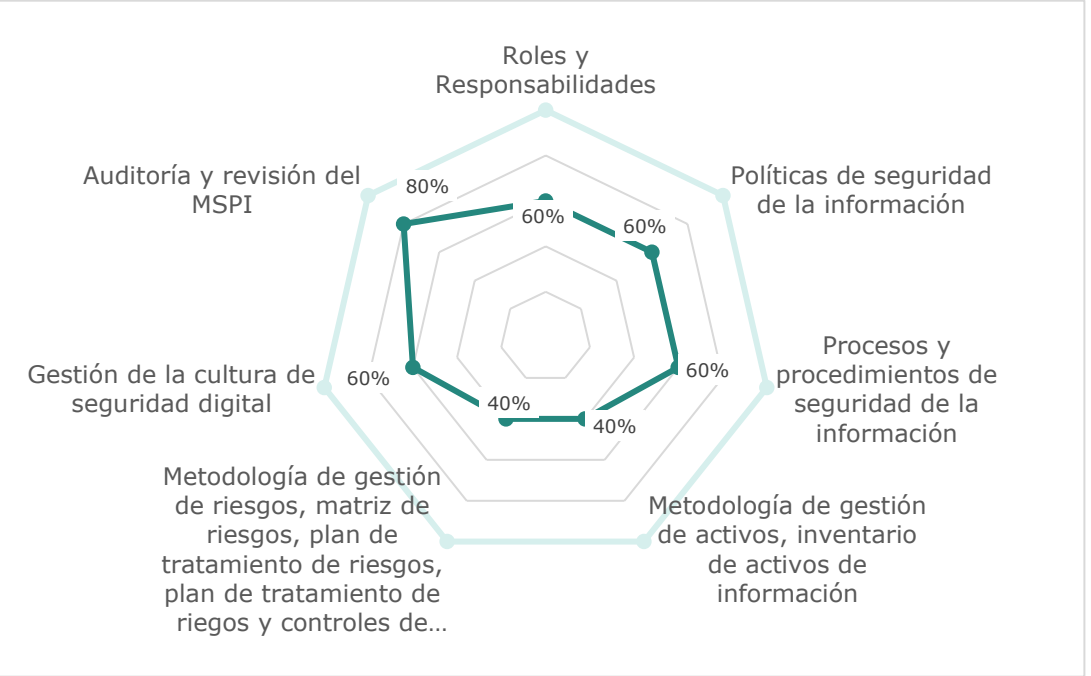

Ilustración 10 Situación actual documentos MSPI del MSPS

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

6.2.1.2. Componentes del MSPI del MSPS

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

Arquitectura de seguridad digital (20%): la adecuada definición, desarrollo y aplicación de una arquitectura de seguridad digital se apoya en los ejercicios de arquitectura empresarial; no se observa la integración de estas dos arquitecturas. No obstante, se cuenta con un conjunto de artefactos que consisten en diagramas de red que identifican componentes de seguridad perimetral y la integración con arquitectura de nube.

Aseguramiento del modelo de interoperabilidad (40%): el MSPS no cuenta con una herramienta estructurada para la interoperabilidad del MSPS, pero sí cuenta con desarrollos a la medida para el intercambio de la información del MSPS con el Sector Salud.

Gestión de incidentes de seguridad (40%): se cuenta con la guía de Gestión de Incidentes, la cual contempla las actividades mínimas requeridas por los lineamientos de MinTIC, no obstante, no hay articulación de la gestión de incidentes entre soporte informático y seguridad de la información.

Privacidad de la información y protección de datos personales (40%): el MSPI está implementado siguiendo los lineamientos del MinTIC.

Mecanismos de autenticación (60%): por medio de directorio activo se gestiona y controla el acceso a servicios de red y aplicaciones, además está implementado 2FA para el acceso a las aplicaciones.

Retención y destrucción final de información (20%): se cuenta con el formato *GSTF09 Borrado seguro de información* para los equipos que se van a dar de baja o en donación, pero no existe un procedimiento o guía con los lineamientos para el borrado seguro de información.

Aseguramiento del proceso de desarrollo de software (20%): el MSPS cuenta con varios documentos con lineamientos para el desarrollo seguro de aplicaciones Web, pese a que no hay lineamientos para el mantenimiento de las aplicaciones cliente-servidor que están en operación.

Gestión segura de terceros y colaboradores (60%): se cuenta con la política de relación con proveedores y se aplica mediante acuerdos de confidencialidad.

Gestión de Continuidad de Recuperación de desastres (40%): el Plan de Recuperación de Desastres del MSPS contempla los servicios de apoyo críticos para el centro de datos principal, esto es misional. No se cuenta con recuperación de los servicios del centro de datos local con los servicios administrativos.

Gestión de vulnerabilidades (60%): el MSPS cuenta con herramientas de escaneo de vulnerabilidades técnicas, sin embargo, no se cuenta con procedimientos formales de gestión de vulnerabilidades, como tampoco hay articulación de actividades entre OTIC y soporte informático en relación con la gestión de vulnerabilidades.

Monitoreo de seguridad y correlación de eventos (40%): se cuenta con el procedimiento de monitoreo de las aplicaciones misionales que operan en la nube pública.

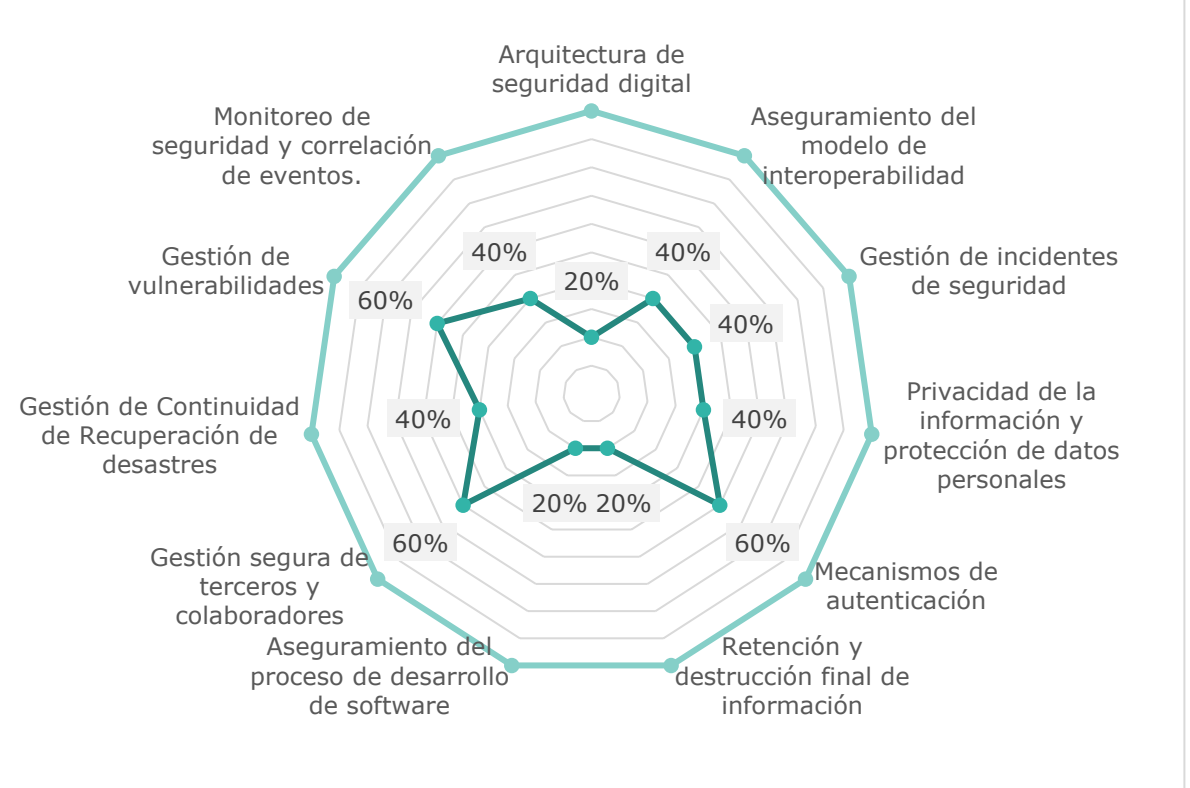

Ilustración 11 Situación actual componentes MSPI del MSPS

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

6.2.1.3. Análisis DOFA del MSPS

Debilidades: en general, se identifica alta rotación del personal de planta, baja interoperabilidad con los sistemas y servicios del sector salud es insuficiente. Aun cuando se ha avanzado en capacitación, muchos colaboradores, usuarios finales y contratistas, aún tienen un nivel bajo de conocimiento sobre la ciberseguridad.

Oportunidades: la evolución de los marcos de trabajo, normativas y mejores prácticas en seguridad de la información y protección de datos, le permite al MSPS adoptar las novedades tan pronto como sean publicadas, como es el caso de la aparición de nuevas tecnologías como blockchain, inteligencia artificial y el aprendizaje automático, que pueden proporcionar soluciones innovadoras para asegurar los datos sensibles de los pacientes y la ciudadanía en general.

Fortalezas: el MSPS tiene el mandato de proteger la privacidad y seguridad de los datos personales de los ciudadanos, lo cual refuerza su compromiso en la

implementación de estándares de seguridad y refuerza el compromiso institucional, así mismo, La experiencia acumulada en la gestión de datos de salud en el entorno nacional ofrece una ventaja en el diseño de sistemas de protección de datos adecuados para el contexto colombiano.

Amenazas: existen dos grupos que ejecutan actividades relacionadas con seguridad digital: a) Gobierno del MSPI en OTIC y b) Soporte Informático en Secretaría General; estos roles y responsabilidades están separados, por lo que no hay una gestión efectiva del MSPI en la articulación de políticas con la aplicación de controles.

El sector salud es un objetivo frecuente de ciberataques, como el ransomware y las filtraciones de datos, representando una amenaza constante para la confidencialidad, integridad y privacidad de los datos personales de los ciudadanos y la continuidad de los servicios.

6.2.1.4. Análisis PESTEL del MSPS

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 Ministerio de Salud. Leyes como la Ley 1581 de 2012 sobre protección de datos personales y la Resolución 500 de 2021 sobre la estrategia de seguridad digital regulan este ámbito, entre otros.

Económico: la suma de recursos económicos asignados para la ciberseguridad y la protección de datos dentro del Ministerio afecta la capacidad de implementar infraestructuras de seguridad robustas. Los recortes presupuestales pueden limitar la efectividad de las políticas de protección de datos.

Social: el alto nivel de conocimiento de las partes interesadas en materia de seguridad y privacidad de la información hace que el entorno sea más exigente. Existe un creciente interés y conciencia por parte de la ciudadanía en torno a sus derechos de privacidad y protección de datos, lo cual incrementa la presión sobre el Ministerio para proteger esta información.

Tecnológico: la integración de diversos sistemas de información de salud con el entorno sectorial puede facilitar la protección y administración de datos, pero también implica riesgos adicionales de seguridad si no se realizan con estándares robustos; la capacidad del Ministerio para implementar tecnologías avanzadas depende de su infraestructura tecnológica actual, la cual puede ser limitada o inadecuada en ciertas áreas.

Ecológico: la adopción de tecnologías de ciberseguridad implica un consumo energético considerable. En el marco de políticas sostenibles, el Ministerio podría considerar la eficiencia energética en sus sistemas de protección de datos. El

Ministerio puede reducir el impacto ambiental relacionado con su infraestructura de TI, promoviendo el uso de tecnologías menos contaminantes, además de extender la migración hacia la nube en lugar de servidores físicos para la infraestructura no misional--.

Legal: las políticas internas del MSPS deben alinearse con las regulaciones nacionales y las mejores prácticas internacionales para garantizar un manejo ético y legal de la información personal, en particular, la Superintendencia de Industria y Comercio (SIC) tiene la facultad de supervisar y sancionar a las instituciones que no cumplan con las normas de protección de datos, lo que implica un riesgo legal significativo en caso de no cumplir con las regulaciones establecidas.

6.2.2. Diagnóstico

Para establecer un diagnóstico de la situación actual del Sistema de Gestión de Seguridad de la Información del Ministerio de Salud y Protección Social, 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 el MSPS y se realizaron entrevistas a los responsables del proceso, lo que permitió obtener una visión integral de la situación actual.

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 aspectos clave del MSPI

- Modelo de Gobierno
- Modelo de Operación
- Gestión de Accesos
- Gestión de Incidentes
- Gestión de la Configuración
- Gestión de Vulnerabilidades
- Acuerdos con Terceros
- Protección de Datos Personales
- Requisitos Legales y Contractuales
- Continuidad
- DRP

- Arquitectura
- Infraestructura
- Borrado Seguro
- Cifrado
- Desarrollo Seguro
- Monitoreo
- Procedimientos
- Respaldos
- Nuevas Tecnologías

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 actual del MSPS. Estas acciones de mejora están plenamente alineadas con los proyectos definidos en la hoja de ruta.

6.2.3.1. Gobierno de Seguridad

Con el análisis de la situación actual del MSPS realizado se exponen a continuación los diferentes aspectos que deben ser considerados para optimizar los controles de seguridad digital existentes:

Fortalecer el modelo de gobernanza del SGSI:

- Reubicando el SGSI para que dependa directamente de la oficina del ministro, dado que el sistema es transversal a toda la organización y no para alguna área en particular, lo que garantiza su independencia y autonomía.
- Incorporando a representantes de los procesos misionales en la toma de decisiones estratégicas. Esto garantizará que los objetivos de seguridad de la información estén alineados con la visión general del Ministerio y se promueva una cultura de seguridad a nivel institucional.

- Fortalecer el modelo de gobernanza de seguridad del Ministerio como líder del sector salud, integrando a los representantes de las entidades del sector para la toma de decisiones transversales y acordando lineamientos para la protección de la información de la ciudadanía.

El modelo de gobierno debe, entre otras actividades, realizar lo siguiente:

- Llevar a cabo una revisión exhaustiva de los procesos de seguridad de la información y realizar los ajustes necesarios para su correcta articulación.
- Incluir todos los procesos, especialmente los misionales, en la evaluación de riesgos del SGSI.
- Revisar las necesidades futuras, considerando el desarrollo de nuevas tecnologías y un entorno socio-político cambiante.
- Ajustar los lineamientos sectoriales para garantizar la protección de la información de la ciudadanía, en especial la compartida con otras entidades.
- Entregar evidencia documentada del funcionamiento del sistema, de acuerdo con los lineamientos del MSPI.
- Revisar y ajustar la articulación con otros sistemas de gestión de tecnología, como COBIT e ITIL v4, para maximizar recursos, así como su integración con el sistema de gestión del MSPS.
- Gestionar más recursos para todas las entidades del sector, basándose en un análisis de riesgos de seguridad sectorial.

6.2.3.2. Arquitectura de seguridad

Realizar la identificación de riesgos de seguridad de la información a partir del ejercicio de Arquitectura empresarial, para mejorar la alineación estratégica del MSPS de acuerdo con las capacidades en seguridad de la información. Asimismo, desarrollar y mantener actualizados todos los artefactos del dominio de seguridad de arquitectura empresarial de acuerdo con los requerimientos del MinTIC.

La arquitectura de seguridad debe apoyar en:

- Diseñar la estrategia general de seguridad de la información alineada con los objetivos estratégicos de la Entidad.

- Gestionar los presupuestos de inversión en tecnologías para mejor la seguridad digital
- 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.
- Garantizar el cumplimiento de las leyes y reglamentos aplicables
- Apoyar la interoperabilidad entre todos los componentes que supervisan la seguridad de la información.

6.2.3.3. Herramientas de seguridad

El SGSI del Ministerio 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 datos 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. 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.

El MSPS debe avanzar en este propósito a medida que se mejoren los niveles de madurez en los controles que se implementen en seguridad digital en los procesos misionales. 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. Capacidad de Recurso Humano en SI

El MSPS debe mejorar la capacidad del recurso humano en seguridad de la información, validando formas de contratación para garantizar como mínimo la estabilidad del equipo que conforma la primera línea de defensa, es decir, los líderes de seguridad de la información. Esta capacidad debe tener en cuenta las competencias para lograr liderazgo en el sector salud y habilidades de trabajo con nuevas tecnologías. Se recomienda validar la capacidad del recurso humano en seguridad de la información para que los procesos del MSPS puedan auto gestionarse y medir la aplicación de los controles de seguridad definidos por el SGSI.

6.2.3.6. Conocimientos en Seguridad de la Información

El SGSI debe desarrollar un plan de mejoramiento en conocimientos en seguridad de la información, que incluya: medición del nivel de conocimientos en seguridad de la información a todos los funcionarios y contratistas; conocimiento y aplicación del proceso de "Revisión por la Dirección"; medición

del nivel de conocimiento y aplicación de los procesos de seguridad de la información.

6.2.3.7. Seguridad de la Información en la Continuidad de Negocio.

El MSPS debe propender para que en el desarrollo del BIA se ejecuten pruebas de funcionamiento periódicas y proveer todos los recursos necesarios, en especial para los servicios de seguridad de la información a fin de no exponer a la entidad a vulnerabilidades durante su ejecución.

6.2.3.8. Seguridad de la Información en Acuerdos con Terceros

Revisar e implementar acuerdos con terceros que incluyan entre otros:

- Colaboración para la contención y gestión de incidentes;
- Auditorias;
- 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 del MSPS, se debe solicitar en los contratos la obligatoriedad de la toma de capacitaciones y aplicación de controles definidos por el SGSI.

6.2.3.9. Controles de los procesos de Seguridad de la Información

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:

- Gestión de Acceso
- Gestión de Vulnerabilidades
- Gestión de Incidentes
- Gestión de Activos de Información
- Gestión de Riesgos

- Gestión de acuerdos con terceros

6.2.3.10. Protección de los Datos Personales.

El SGSI del MSPS debe propender por la mejora de la protección de datos personales de los ciudadanos en todas las regiones del país, por ello, debe establecer con especial atención, puntos de control para la verificación y medición de la aplicación de los procedimientos establecidos para la recolección y gestión de los datos personales. Estos resultados deben ser dados a conocer a la ciudadanía para generar confianza en la entrega de datos.

6.2.3.11. Plan de mejora.

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.

6.2.4. Análisis de Maduración

La metodología para identificar el estado actual de los principales lineamientos y aspectos clave del MSPI del Ministerio, está completamente alineada con las directrices de MinTIC y hace uso del marco de referencia para niveles de madurez establecido por Gartner Inc.

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 2 Niveles de maduración Gartner

Fuente: Gartner

6.2.4.1. Análisis de Maduración frente al MSPI

En la revisión frente a los lineamientos del MSPI se encontraron en un estado de implementación "repetible" (según los niveles establecidos en el documento diagnóstico de seguridad institucional y sectorial) los siguientes lineamientos:

- 7.3.1 Identificación de activos de información;
- 7.3.2 Valoración de riesgos;
- 7.3.3 Plan de tratamiento de riesgos; y
- 8.2 Evaluación de riesgos

Estos resultados se deben a la falta de involucramiento de todos los procesos de la organización, especialmente los procesos misionales, en la gestión de riesgos del SGSI. Esta oportunidad de mejora, sumada a los problemas de articulación identificados entre el gobierno de seguridad de la información y la seguridad informática, se reflejó en las evaluaciones de los numerales:

- 9.1.3 Revisión por la dirección.
- 10.1 Mejora.

Por otro lado, se evidenciaron fortalezas en los numerales:

- 7.1.1 Comprensión de la organización y su contexto.
- 7.1.2 Necesidades y expectativas de los interesados.

En estos casos, se destaca un buen conocimiento del contexto del sector salud y de las necesidades y expectativas de los interesados, como la ciudadanía.

A continuación, se presenta el resumen del diagnóstico en una gráfica radial que muestra los resultados frente a los lineamientos del MSPI.

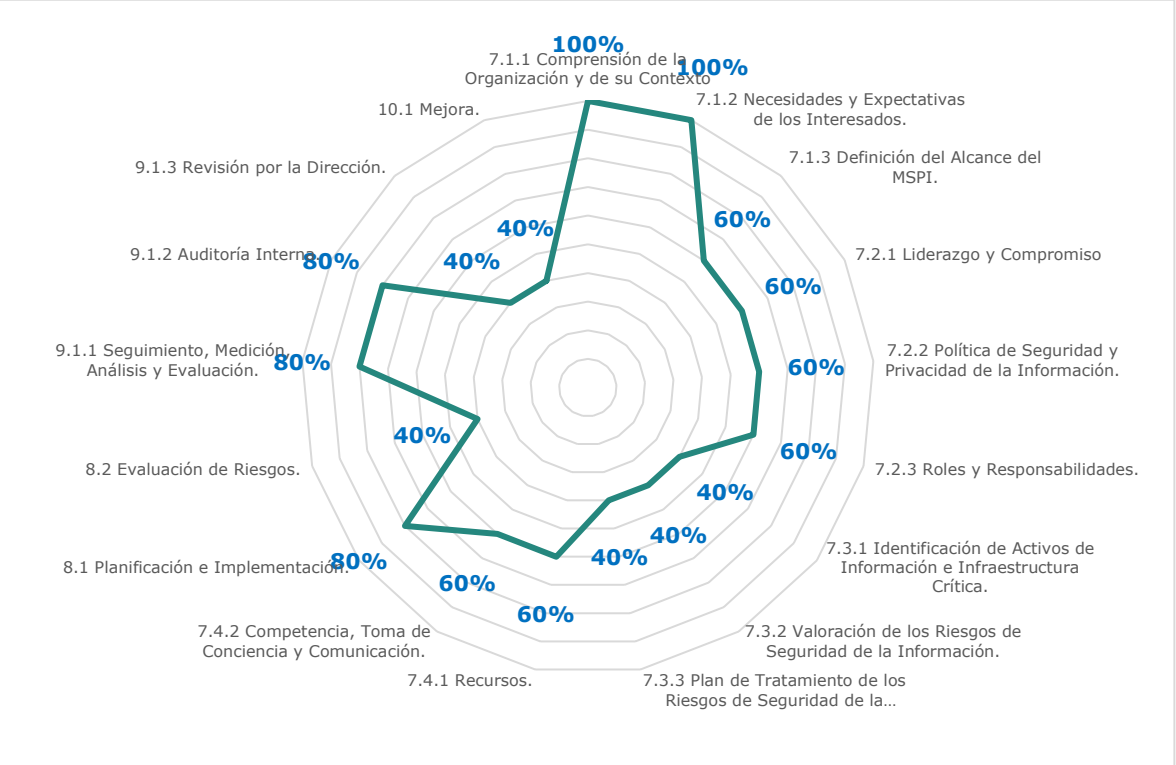

Ilustración 12 Diagnóstico MSPS Frente al MSPI

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

6.2.4.2. Análisis de Maduración frente a Controles Clave de SI

En la revisión de aspectos clave de seguridad de la información, se identificaron las siguientes oportunidades de mejora:

Proceso de desarrollo seguro:

Aunque el MSPS cuenta con políticas y lineamientos para el desarrollo seguro, su adopción en el desarrollo de nuevos sistemas de información es insuficiente. Esto deja vulnerables algunas aplicaciones frente a posibles acciones de intrusos informáticos. Además, se debe considerar la incorporación de herramientas de escaneo adicionales a las actuales, como aquellas para análisis de aplicaciones estáticas y análisis de composición del software, garantizando así el ciclo de vida completo de las aplicaciones.

Retención y destrucción de información

Se evidenciaron debilidades importantes en este proceso. Aunque el Ministerio dispone de un formato para este fin, no existe una guía o procedimiento con lineamientos específicos para el borrado seguro de la información.

En conclusión, es necesario mejorar la implementación de todos los controles de seguridad, validando el ciclo de vida de cada servicio gestionado por el SGSI.

A continuación, se presenta el resumen diagnóstico en una gráfica radial que muestra los resultados frente a los aspectos clave de seguridad de la información.

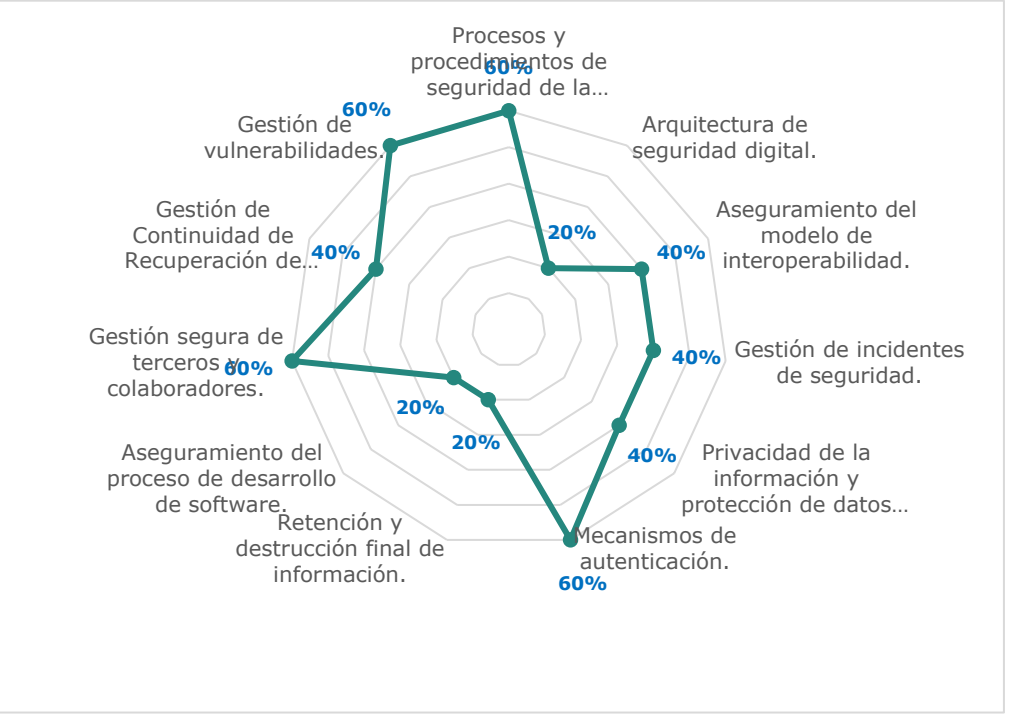

Ilustración 13 Diagnóstico MSPS-Controles Clave de Seguridad de la Información

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

Para ver el detalle de las observaciones frente a 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. Proyectos

6.3.1. 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 institucional. 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	INI001
Nombre de la Iniciativa	Modelo de Gobernanza
Descripción de la Iniciativa	Diseñar e implementar un modelo de gobernanza que gestione apropiadamente los lineamientos de seguridad digital con la gestión de los componentes de seguridad perimetral on-premise y nube pública para el MSPS.
Rubro presupuestal	$ 589.500.000,00
Plazo	Menos de 6 meses para su implementación

Tabla 3 Iniciativa Institucional INI001

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

ID Iniciativa	INI002
Nombre de la Iniciativa	Plan de Recuperación de Desastres - BCP
Descripción de la Iniciativa	Adoptar el plan de recuperación de desastres - BCP producto de la consultoría del Contrato 1588 en el frente BCP que contemple los servicios misionales para el centro de datos principal y servicios de nube pública.
Rubro presupuestal	$ 594.000.000,00
Plazo	Menos de 6 meses para su implementación

Tabla 4 Iniciativa Institucional INI002

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

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

Tabla 5 Iniciativa Institucional INI003

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

ID Iniciativa	INI004
Nombre de la Iniciativa	Herramienta de Cifrado
Descripción de la Iniciativa	Contratar una herramienta de cifrado que asegure la protección de datos personales con alcance a todos los procesos del MSPS, 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 6 Iniciativa Institucional INI004

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

ID Iniciativa	INI002
Nombre de la Iniciativa	Cultura y apropiación del SI
Descripción de la Iniciativa	Diseñar e implementar una campaña institucional que propenda por la apropiación de la cultura de seguridad de la información y protección de datos personales con alcance al todos los procesos del MSPS.
Rubro presupuestal	$ 582.000.000,00
Plazo	Menos de 6 meses para su implementación

Tabla 7 Iniciativa Institucional INI002

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

ID Iniciativa	INI004
Nombre de la Iniciativa	Gestión de Activos de Información
Descripción de la Iniciativa	Fortalecer la gestión de activos mediante la identificación, clasificación y valoración de activos de información y datos personales, en todos los procesos del MSPS.
Rubro presupuestal	$ 329.608.000,00
Plazo	Menos de 6 meses para su implementación

Tabla 8 Iniciativa Institucional INI004

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

ID Iniciativa	INI007
Nombre de la Iniciativa	Gestión de Riesgos de SI
Descripción de la Iniciativa	Fortalecer la gestión de riesgos para los activos de información identificados, que incluya valoración y planes de tratamiento, para todos los procesos del MSPS.
Rubro presupuestal	$ 624.000.000,00
Plazo	Menos de 6 meses para su implementación

Tabla 9 Iniciativa Institucional INI007

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

6.3.2. 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 su postura de seguridad.

Descripción y Evaluación de Iniciativas

1. **Gestión de Activos de Información (INI006)**
    - **Descripción**: Fortalecer la gestión de activos mediante la identificación, clasificación y valoración de activos de información y datos personales, en todos los procesos del MSPS.
    - **Duración**: Corto plazo.
    - **Costo Estimado**: $329.608.000.
    - **Evaluación**: Fundamental para establecer una base sólida que permita gestionar y proteger adecuadamente los diferentes tipos de información manejados por el ministerio.

2. **Gestión de Riesgos de SI (INI007)**

    - **Descripción**: Fortalecer la gestión de riesgos para los activos de información identificados, que incluya valoración y planes de tratamiento, para todos los procesos del MSPS.
    - **Duración**: Corto plazo.
    - **Costo Estimado:** $624.000.000.
    - **Evaluación**: Crucial para identificar y mitigar riesgos potenciales, asegurando que las inversiones en seguridad sean efectivas y alineadas con las amenazas reales.

3. **Modelo de Gobernanza (INI001)**

    - **Descripción:** Diseñar e implementar un modelo de gobernanza que gestione apropiadamente los lineamientos de seguridad digital con la gestión de los componentes de seguridad perimetral on-premise y nube pública para el MSPS.
    - **Duración:** Corto plazo.
    - **Costo Estimado:** $589.500.000.
    - **Evaluación:** Vital para asegurar una gestión coherente y unificada de la seguridad en todas las plataformas y entornos operativos del MSPS.

4. **Modelo de Seguridad y Privacidad de la Información (INI003)**

    - **Descripción:** Planificar y desarrollar el Modelo de Seguridad y Privacidad de la Información - MSPI con alcance a todos los procesos de negocio del MSPS.
    - **Duración:** Largo plazo.
    - **Costo Estimado:** $834.000.000.
    - **Evaluación:** Importante para garantizar que todos los procesos de negocio estén alineados con las mejores prácticas de seguridad y privacidad, promoviendo una cultura organizacional orientada a la protección de la información.

5. **Plan de Recuperación de Desastres - BCP (INI002)**

    - **Descripción:** Adoptar el plan de recuperación de desastres - BCP producto de la consultoría del Contrato 1588 en el frente BCP que

contemple los servicios misionales para el centro de datos principal y servicios de nube pública.

- **Duración:** Corto plazo.
- **Costo Estimado:** $594.000.000.
- **Evaluación:** Esencial para asegurar la resiliencia operativa del ministerio ante posibles incidentes que puedan interrumpir las operaciones críticas.

6. **Herramienta de Cifrado (INI004)**
    - **Descripción:** Contratar una herramienta de cifrado que asegure la protección de datos personales con alcance a todos los procesos del MSPS, considerando el resultado de la identificación y clasificación de activos de información y datos personales.
    - **Duración:** Largo plazo.
    - **Costo Estimado:** $1.074.000.000.
    - **Evaluación:** Crucial para proteger la confidencialidad e integridad de la información sensible, reduciendo significativamente el riesgo de brechas de datos.
7. **Cultura y apropiación del SI (INI005)**
    - **Descripción:** Diseñar e implementar una campaña institucional que propenda por la apropiación de la cultura de seguridad de la información y protección de datos personales con alcance a todos los procesos del MSPS
    - **Duración:** Corto plazo.
    - **Costo Estimado:** $582.000.000.
    - **Evaluación:** Fundamental para involucrar a todos los funcionarios en las prácticas de seguridad, fortaleciendo la defensa organizacional contra amenazas internas y externas.

En este sentido, el MSPS debe tener en cuenta las siguientes consideraciones:

1. **Priorización de Iniciativas de Corto Plazo:** Las iniciativas con una duración a corto plazo representan una inversión significativa y abordan riesgos inmediatos. Implementarlas primero permitirá establecer una

base robusta de seguridad, facilitando la ejecución de proyectos de largo plazo.

2. **Inversión en Tecnologías Críticas:** La implementación de modelos de cifrado y gestión de riesgos, aunque costosos, son esenciales para proteger datos sensibles y asegurar la continuidad operativa, justificando plenamente su inversión.

3. **Cultura de Seguridad Organizacional:** La campaña de cultura de seguridad es indispensable para garantizar que todos los miembros del MSPS comprendan y adopten las mejores prácticas de seguridad, lo que potenciará la efectividad de todas las demás iniciativas.

4. **Gestión Integral y Gobernanza:** Un modelo de gobernanza integrado asegura una gestión coherente y eficiente de la seguridad en todos los niveles y plataformas, promoviendo una postura de seguridad unificada y coordinada.

5. **Planificar la Implementación de Iniciativas de Largo Plazo:** Desarrollar un cronograma detallado para la implementación del MSPI y el modelo de cifrado, asegurando una asignación equilibrada de recursos financieros y humanos a lo largo de los próximos años.
6. **Asignación Estratégica de Recursos:** Asegurar que el presupuesto esté adecuadamente distribuido para cubrir tanto las iniciativas de corto como de largo plazo, evitando sobrecargas financieras en periodos específicos y garantizando la sostenibilidad del plan de seguridad.
7. **Monitoreo y Evaluación Continua:** Establecer mecanismos de seguimiento y evaluación para cada iniciativa, utilizando indicadores clave de rendimiento (KPI) que permitan medir su progreso y efectividad, y realizar ajustes según sea necesario.
8. **Capacitación Continua del Personal:** Invertir en programas de formación y sensibilización para todo el personal del MSPS, asegurando que comprendan la importancia de la seguridad de la información y sepan cómo aplicar las políticas y procedimientos establecidos.
9. **Adopción de Tecnologías Emergentes:** Mantenerse actualizado con las últimas tendencias y avances en ciberseguridad, evaluando e integrando tecnologías innovadoras que puedan mejorar la capacidad de detección y respuesta ante incidentes de seguridad.
10. **Desarrollo de Planes de Contingencia:** Elaborar y mantener actualizados planes de contingencia que permitan al MSPS responder eficazmente ante incidentes de seguridad, minimizando el impacto en las operaciones críticas.

El MSPS está en una posición estratégica para fortalecer significativamente su seguridad de la información mediante la implementación de las iniciativas propuestas. Al priorizar las acciones de corto plazo que abordan riesgos inmediatos y establecer una base sólida para proyectos de largo plazo, el ministerio puede asegurar la protección de sus activos informacionales y asegurar la continuidad de sus operaciones.

6.3.3. Hoja de Ruta

La hoja de ruta del PESI institucional detalla la planificación estratégica para la implementación de proyectos clave relacionados con la transformación digital y la seguridad de la información en el sector salud. Distribuida en etapas trimestrales hasta 2028, tal como se establece en el documento *MSPS_Hoja de Ruta PESI Institucional,* esta herramienta permite visualizar los plazos, las inversiones previstas y las acciones prioritarias, asegurando un enfoque estructurado y alineado con los objetivos organizacionales. Cada proyecto está diseñado para fortalecer la infraestructura tecnológica, garantizar la gobernanza de datos y promover una cultura de protección de la información.

HOJA DE RUTA PESI INSTITUCIONAL

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.

INICIATIVAS	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
INI006 - Gestión de Activos de Información																																															
INI007 - Gestión de Riesgos de SI																																															
INI001 - Modelo de Gobernanza																																															
INI003 - Modelo de Seguridad y Privacidad de la Información																																															
INI002 - Plan de Recuperación de Desastres - BCP																																															
INI004 - Herramienta de Cifrado																																															
INI005 - Cultura y apropiación del SI																																															
	$ 1.897.108.000,00												$ 1.536.000.000,00												$ 1.131.000.000,00																							
	Proyectos en curso 4												Proyectos en curso 3												Proyectos en curso 2												Proyectos en curso 0											
	TOTAL ESTIMADO EN PROYECTOS DE INVERSIÓN $ 4.564.108.000,00																																														

Ilustración 14 Hoja de Ruta PESI Institucional

Fuente: elaboración propia UT MYQ ALINATECH PETI 2024

6.4. Estrategias

6.4.1. Iniciativas vs. Objetivos Estratégicos de SI

La relación entre los Objetivos estratégicos de Seguridad de la Información y las Iniciativas de Seguridad de la Información para el Ministerio de Salud y Protección Social (MSPS) demuestra una coherencia estratégica que abarca diversas áreas clave para fortalecer la seguridad y protección de los activos de información de la entidad. Cada objetivo está respaldado por iniciativas específicas que, en conjunto, conforman un marco integral para abordar las distintas dimensiones de la seguridad de la información.

El **OBJ1**, centrado en la gestión de los activos de información, encuentra su apoyo en varias iniciativas. La **INI006**, que desarrolla una estrategia para la clasificación de activos de información y datos personales, es fundamental para identificar y valorar adecuadamente los activos, lo que permite implementar medidas de protección adecuadas. Asimismo, la **INI001**, que implementa un modelo de gobierno integrado, y la **INI003**, que desarrolla el Modelo de Seguridad y Privacidad de la Información (MSPI), aseguran una gestión holística de los activos, incorporando políticas y procedimientos que garantizan la protección continua de la información. La **INI004**, que introduce un modelo de cifrado para bases de datos, añade una capa adicional de seguridad, protegiendo datos sensibles contra accesos no autorizados y asegurando la confidencialidad e integridad de la información manejada.

En relación con el **OBJ2**, que se enfoca en la gestión de los riesgos de seguridad de la información, las iniciativas **INI006** e **INI007** son esenciales. La **INI006** no solo clasifica los activos, sino que también permite una mejor identificación y valoración de los riesgos asociados a cada activo, mientras que la **INI007** se dedica específicamente a la gestión de estos riesgos mediante la implementación de planes de tratamiento. Estas iniciativas aseguran que se adopten los controles necesarios para mitigar los riesgos identificados, contribuyendo así a la sostenibilidad operativa del ministerio. Además, tanto la **INI001** como la **INI003** integran la gestión de riesgos dentro de un marco de gobernanza más amplio, facilitando una respuesta coordinada y eficiente ante las amenazas emergentes.

El **OBJ3**, orientado a fortalecer la cultura de seguridad de la información, está respaldado principalmente por las iniciativas **INI001**, **INI003** e **INI005**. La **INI005**, que diseña una campaña institucional para promover la cultura de seguridad, es crucial para fomentar una mentalidad de seguridad entre todos los colaboradores del MSPS. Esta campaña asegura que cada miembro de la organización esté consciente de las políticas de seguridad y de la importancia de proteger los datos personales y la información sensible. Las iniciativas **INI001**

y **INI003** complementan esta campaña al establecer modelos de gobernanza y seguridad que integran la cultura de seguridad en todos los procesos de negocio, garantizando así una adopción generalizada y sostenida de las prácticas de seguridad.

Respecto al **OBJ4**, que se enfoca en mantener la seguridad de la información durante interrupciones tecnológicas, las iniciativas **INI001**, **INI003** e **INI002** juegan roles fundamentales. La **INI002**, que implementa un plan de recuperación de desastres, asegura que los servicios misionales puedan continuar operando incluso ante fallos en la infraestructura tecnológica. Esto es esencial para mantener la disponibilidad y la integridad de la información crítica del ministerio. Las iniciativas **INI001** y **INI003** fortalecen este objetivo al establecer mecanismos de gobernanza y modelos de seguridad que incorporan planes de continuidad del negocio y recuperación ante desastres, garantizando que la seguridad de la información no se vea comprometida durante cualquier interrupción tecnológica.

Finalmente, el **OBJ5**, centrado en la gestión de eventos e incidentes de seguridad de la información, se apoya en varias iniciativas clave, incluyendo **INI001**, **INI003**, **INI002**, **INI004** e **INI005**. La **INI001** y la **INI003** establecen un marco robusto de gobernanza y seguridad que facilita la detección y respuesta a incidentes de seguridad. La **INI002** contribuye a este objetivo al asegurar que existen planes de continuidad que permiten una rápida recuperación tras cualquier incidente. La **INI004**, al implementar un modelo de cifrado, protege los datos sensibles contra accesos no autorizados, reduciendo la probabilidad de incidentes de seguridad relacionados con la información confidencial. Por último, la **INI005**, al promover una cultura de seguridad, garantiza que todos los colaboradores estén preparados para identificar y responder adecuadamente a los incidentes, fortaleciendo así la capacidad del ministerio para enfrentar amenazas y ataques informáticos de manera efectiva.

En conjunto, las iniciativas propuestas no solo apoyan cada uno de los objetivos estratégicos de seguridad de la información, sino que también interactúan de manera sinérgica para crear un entorno de seguridad robusto y resiliente. La implementación de estas iniciativas asegura que el MSPS pueda gestionar eficientemente sus activos de información, mitigar riesgos, fomentar una cultura de seguridad, mantener la continuidad operativa durante interrupciones y gestionar de manera efectiva los incidentes de seguridad. Este enfoque integral permite al ministerio proteger de manera efectiva la integridad, confidencialidad y disponibilidad de su información, alineándose con las mejores prácticas y estándares internacionales en seguridad de la información.

6.4.2. Iniciativas vs. Planes de Política de Seguridad Digital

En este aparte se realiza un análisis sobre el documento *"MSPS_Catálogo de Iniciativas Institucional. 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:** INI007, INI001, INI003, INI005. Estos proyectos son esenciales para lograr una cobertura integral de la seguridad digital, abarcando desde la gestión de riesgos y la gobernanza hasta la promoción de una cultura de seguridad.

- **Proyectos de Media Prioridad**: INI006, INI002, INI004. 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 INI006, INI007, INI001, INI002, e INI005 permitirá obtener beneficios inmediatos, como la clasificación de activos, gestión de riesgos, establecimiento de modelos de gobernanza y campañas de concientización.

- **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:** INI003 e INI004 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 gestión de riesgos, 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 gobernanza y cifrado de datos.

4. Fomento de una Cultura de Seguridad Digital

- **Importancia de INI005:** 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 y la confianza en los servicios digitales.

6.4.3. 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.

6.5. Medición e Indicadores

La medición del presente plan, se enfoca en la evaluación del "*Tablero de Indicadores PESI INSTITUCIONAL"*, diseñado para monitorear y medir el desempeño de las iniciativas del Plan Estratégico de Seguridad de la Información (PESI) INSTITUCIONAL. 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 en el Ministerio de Salud y Protección Social (MSPS).

9. 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.

10. 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.

11. 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.

12. 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.

13. Eficacia y Eficiencia en la Gestión de Proyectos

- Eficacia en la Gestión del Riesgo: El indicador IND.PESI.Inst.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.Inst.003 y IND.PESI.Inst.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.

14. 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, gobernanza 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 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.

- Con respecto a la cobertura Integral de los Proyectos, 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.

- El documento refleja un esfuerzo integral para abordar los retos de seguridad en el sector salud. Sin embargo, el éxito del Plan Estratégico dependerá de la capacidad del MSPS para integrar completamente sus iniciativas en todos los niveles organizacionales, reforzar la cultura de seguridad y adaptarse proactivamente a un entorno de amenazas en constante evolución. Un énfasis en la gobernanza, la capacitación y el uso de tecnologías avanzadas puede posicionar al MSPS como un referente en seguridad digital en el sector público.

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. Axelos. (2019). *ITIL® 4: A Guide to the ITIL® Service Value System.* Axelos. Recuperado de https://www.axelos.com

International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 - Information security, cybersecurity, and privacy protection — Information security management systems — Requirements.* Recuperado de https://www.iso.org

Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). (2021). *Resolución 500 de 2021: Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad como habilitador de la Política de Gobierno Digital.* Diario Oficial No. 52.181. Recuperado de https://www.mintic.gov.co

Presidencia de la República de Colombia. (2022). *Decreto 767 de 2022: Por el cual se establecen los lineamientos generales de la política de Gobierno*

Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015. Diario Oficial No. 52.294. Recuperado de https://www.mintic.gov.co

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_Institucional

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

MSPS_Acta constitución proyecto_INI001_institucional

MSPS_Acta constitución proyecto_INI003_Institucional

MSPS_Acta Constitución Proyecto_INI002_Institucional

MSPS_Acta constitución proyecto_INI004_Institucional

MSPS_Acta Constitución Proyecto_INI005_Institucional

MSPS_Acta constitución proyecto_INI006_Institucional

MSPS_Ficha y catálogo de gastos sobre la Operación de SI_Institucional

MSPS_Hoja de Ruta PESI_Institucional

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.

Termino	Definición
MinTIC	Ministerio de Tecnologías de la Información y las Comunicaciones. Entidad gubernamental de Colombia 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 10 Glosario
Fuente: elaboración propia UT MYQ ALINATECH PETI 2024