PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PESI)

2024-2026

OIDT

Bogotá, Abril de 2024

Contenido

1. OBJETIVO

Optimizar el Plan de Seguridad y Privacidad de la Información del INM con el fin de alinearse con la estrategia de Gobierno en línea de Ministerio TIC, y la norma de seguridad ISO27001:2022 de tal forma que se establezcan los controles necesarios para mantener la confidencialidad, integridad y disponibilidad de la información del INM a partir de la implementación de estrategias de seguridad digital definidas en este documento para la vigencia 2024-2026.

1.1. OBJETIVOS ESPECÍFICOS

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

2. ALCANCE

El Plan Estratégico de Seguridad de la Información busca la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la entidad, cubriendo el alcance definido dentro de la Política General de Seguridad de la Información del INM, donde se indica que se incluyen todos los procesos de la entidad.

Este plan inicia con la presentación del diagnóstico del estado actual de la seguridad de la información en el INM, continúa con los proyectos establecidos para cada estrategia de seguridad y finaliza con el cronograma y presupuesto.

3. ABREVIATURAS O SÍMBOLOS

INM: Instituto Nacional de Metrología

MinTic: Ministerio de las telecomunicaciones

SGSI: Sistema de gestión de seguridad de la información

PESI: Plan Estratégico de seguridad de la información

4. DEFINICIONES

- **Activos**

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Control**

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Riesgo**

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información**

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI**

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000.

5. MARCO NORMATIVO

- Decreto 612 de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.

- Resolución 500 de 2021. “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- NTC/ISO 27001:2022

6. CONTENIDO PRINCIPAL

La seguridad y privacidad de la información, es un componente transversal a la Estrategia de Gobierno en línea. Este va alineado con la implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos del INM.

El INM ha avanzado en la implantación de este modelo de seguridad y el objetivo es seguir madurándolo en la vigencia 2024-2026, cumpliendo con el ciclo del modelo de seguridad y privacidad de la información, donde se enfatiza en una mejora continua. Este modelo se está implantando apoyado también en el estándar de seguridad ISO 27001:2022.

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

Para establecer el estado actual, el INM ha ejecutado dos diagnósticos en el primer trimestre de 2024. Uno basado en el instrumento de medición propuesto por el MinTIC y otro basado en los controles de la norma ISO27001:2022, los cuales se presentan a continuación:

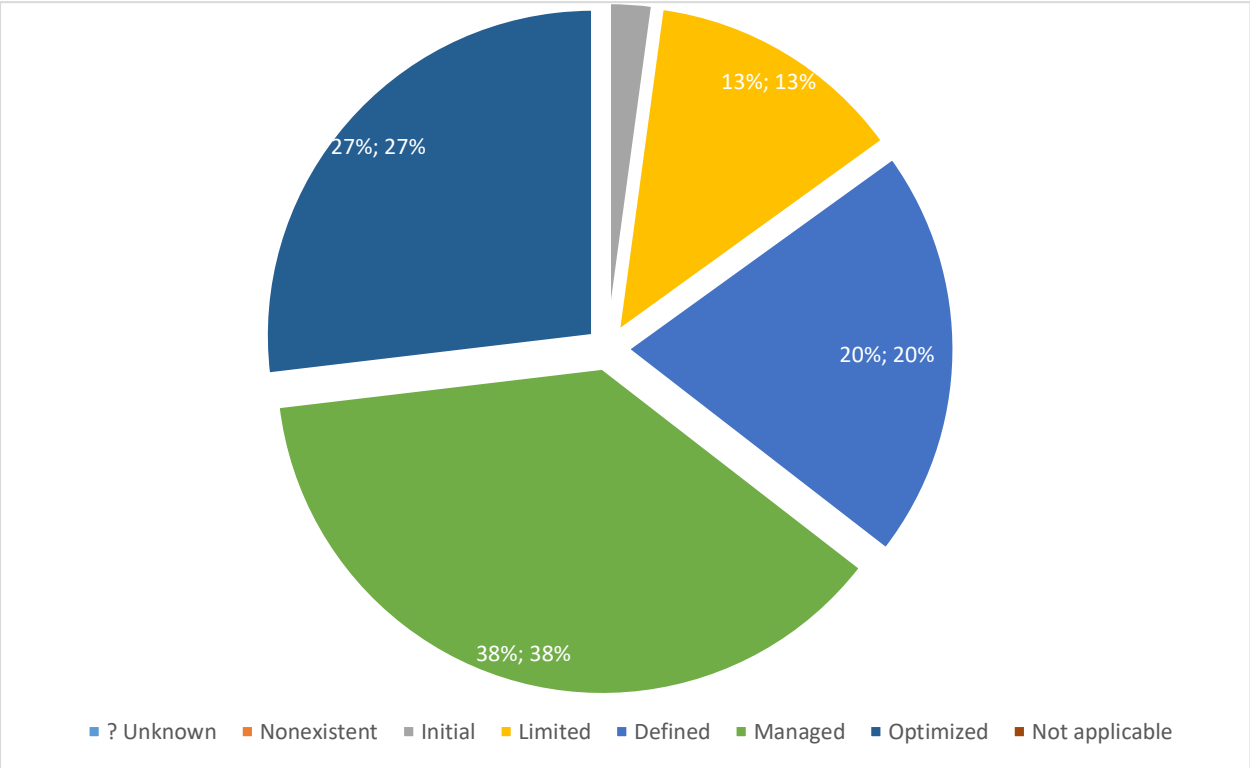
a. Estado del SGSI basado en el instrumento de medición del MSPI

No.	DOMINIO	Calificación Actual	Calificación Objetico	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	Políticas de seguridad de la información	100	100	OPTIMIZADO
A.6	Organización de la seguridad de la información	80	100	GESTIONADO
A.7	Seguridad de los Recursos Humanos	69	100	GESTIONADO
A.8	Gestión de Activos	73	100	GESTIONADO

A.9	Control de Acceso	83	100	OPTIMIZADO
A.10	Criptografía	40	100	REPETIBLE
A.11	Seguridad Física del entorno	83	100	OPTIMIZADO
A.12	Seguridad de las operaciones	72	100	GESTIONADO
A.13	Seguridad de las comunicaciones	74	100	GESTIONADO
A.14	Adquisición, desarrollo y mantenimiento de sistemas	72	100	GESTIONADO
A.15	Relación con los proveedores	40	100	REPETIBLE
A.16	Gestión de incidentes de Seguridad de la Información	94	100	OPTIMIZADO
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	80	100	GESTIONADO
A.18	Cumplimiento	60	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		**73**	**100**	**GESTIONADO**

b. Estado del SGSI basado en el avance de implementación de los controles ISO27001:2022

ESTADO DE LOS CONTROLES DE SEGURIDAD



Los criterios de medición son los siguientes:

ISO/IEC 27001:2022 ISMS		ISO 27001:2013 ANEXO A	
Estado	**Criterio**	**Estado**	**Criterio**
No Aplica	No aplica.	No Aplica	No aplica.
Inexistente	Falta total de políticas, procedimientos, controles, etc. reconocibles.	Inexistente	Total falta de cualquier proceso reconocible.
Inicial	El desarrollo apenas ha comenzado y requerirá un trabajo significativo para cumplir con los requisitos.	Inicial	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
Limitado	Se ha hecho algún progreso, pero aún no se ha completado su implementación	Repetible	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.

Definido	El control está definido o documentado, aunque faltan detalles y/o aún no se implementa	Efectivo	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.
Administrado	El desarrollo está completo, el proceso/control ha sido implementado, documentado y está operando	Gestionado	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.
Optimizado	El requerimiento se cumple completamente, está operando completamente como se esperaba, se está monitoreando y mejorando activamente, y hay evidencia sustancial para demostrar todo eso a los auditores.	Optimizado	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.

Haciendo el análisis de los diagnósticos, lo proyectado es que todos los controles vayan hacia el estado administrado y optimizado. Por lo tanto, en el INM se aprecia que en la vigencia anterior se ha logrado un avance significativo en la madurez hacia estos niveles óptimos.

El INM ha trabajado en la madurez del SGSI aplicando procedimientos, instructivos, sensibilizaciones en seguridad, etc. Los controles en los que se ha trabajado y madurado son de estos temas, como se observa en la gráfica Brecha anexo A ISO27001:2013.

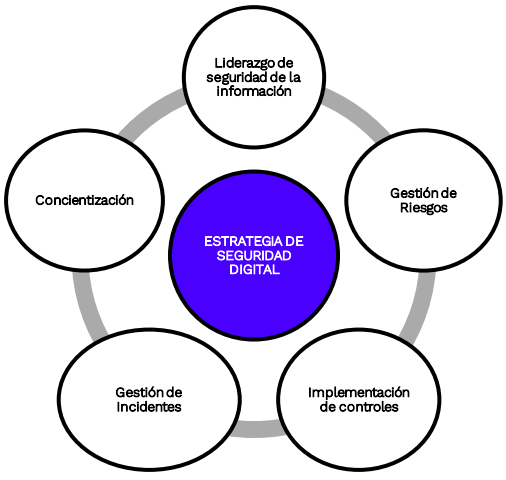
- Políticas de seguridad de la información
- Activos de información
- Control de accesos
- Incidentes de seguridad de la información
- Desarrollo de software
- Seguridad en redes
- Backups
- Documentación de la operación de OIDT
- Gestión de capacidad
- Gestión de riesgos de seguridad de la información

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

6.2 ESTRATEGIA DE SEGURIDAD DIGITAL

EL INM establece una estrategia de seguridad digital en la que integra los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y el procedimiento de gestión de incidentes que ha establecido. Adicionalmente el INM trabaja en su SGSI basado en el estándar de seguridad ISO27001:2022.

Por tal motivo, el INM enfoca su PESI en las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



6.3 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

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

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información mediante la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados, pues simulan la implementación de controles de seguridad para tratarlos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

6.4 PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, el INM define los siguientes proyectos y/o actividades, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI) en la vigencia 2024-2026:

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	Capacitar en seguridad de la información a los roles de seguridad de la información de la empresa.	Certificado o evidencia de participación en las capacitaciones
	Actividades para madurar los roles de seguridad de la información y su gestión	Documento de roles y responsabilidades del INM actualizado
	Culturizar a los líderes en su responsabilidad dentro de la seguridad de la información.	Sesiones y material de sensibilización de seguridad en los líderes.
Gestión de riesgos	Gestión de riesgos y planes de tratamiento de riesgos de seguridad de la información	4 Informes de seguimiento a de riesgos de seguridad de la información
	Uso y apropiación de la gestión de riesgos de seguridad de la información del INM.	Piezas comunicativas enviadas por intranet
	Automatización de la gestión de riesgos de seguridad de la información.	
	Optimización y maduración de la gestión de riesgos de seguridad de la información	Gestión de riesgos de seguridad en una aplicación de gestión de riesgos

		Documento con la metodología de riesgos Matriz de riesgos de seguridad de la información actualizada y aprobada por CIGD
Concientización	Desarrollo de actividades de uso y apropiación del Modelo de Seguridad y Privacidad de la Información	1. Plan de capacitación y socialización de seguridad y privacidad de la información 2. Evidencias de las capacitaciones y socialización realizadas.
Implementación de controles	**Implementación de controles de la norma ISO 27001:2022:** **Elaboración de documentación en el SGSI** Políticas de seguridad en contratos de proveedores Gestión de la configuración Políticas de criptografía Procedimiento de gestión del cambio Políticas de devolución y disposición segura de activos de información Políticas de gestión de Medios móviles Gestión del Filtrado URL Optimización de documentos de gestión humana y contratación Documentación de sincronización de relojes DRP	Plan de trabajo con controles especificados Procedimientos, documentos actualizados. Documentos con políticas de seguridad en gestión de TI

	Políticas de seguridad física	
	Implementación de herramientas de ciberseguridad:	
	Implementación y gestión de infraestructura de redes, NAC y SIEM	
	Implementación y gestión de SOC	
	Implementación y gestión de herramienta de inteligencia de amenazas	
	Optimizar políticas de seguridad en office 365 y nube	
	Implementación del SGSI en una herramienta colaborativa	
	Remediación de vulnerabilidades	
		Herramientas implementadas y documentación elaborada
	Mantenimiento de SGSI	
	Desarrollo de software	
	Remediación de vulnerabilidades y retest a la plataforma de TI	
	Validaciones de controles de accesos	
	Actualización de matriz de activos de información	
	Auditoría al SGSI	
	Gestión de los hallazgos de auditoría y calidad que se relacionen con Seguridad y privacidad de la información	SGSI en herramienta colaborativa

	Evaluación el estado de madurez del SGSI	
		Documentos con políticas de seguridad en gestión de TI
		Matriz activos actualizada, aprobada y publicada
		Informe de auditoría
		Hallazgos cerrados en herramienta de gestión
		Informe del estado del SGSI
		Diagnóstico SGSI
Gestión de incidentes de seguridad	Desarrollar actividades de uso y apropiación del procedimiento de gestión de incidentes para el personal involucrado y de cómo reportar incidentes para todo el personal	Plan de capacitación y socialización de seguridad y privacidad de la información
		Evidencias de las capacitaciones en gestión de incidentes
	Optimización del procedimiento de gestión de incidentes	
		Procedimiento de gestión de incidentes actualizado

7. CRONOGRAMA

<table>
<tr><th>ESTRETEGIA</th><th>TEMA</th><th colspan="4">AÑO 2024</th><th colspan="4">AÑO 2025</th><th colspan="4">AÑO 2026</th></tr>
<tr><td></td><td></td><td>TRIM. 1</td><td>TRIM. 2</td><td>TRIM. 3</td><td>TRIM. 4</td><td>TRIM. 1</td><td>TRIM. 2</td><td>TRIM. 3</td><td>TRIM. 4</td><td>TRIM. 1</td><td>TRIM. 2</td><td>TRIM. 3</td><td>TRIM. 4</td></tr>
<tr><td></td><td>Diagnóstico estado seguridad de la información</td><td>Actualización anual Diagnóstico del estado actual del SGSI del INM</td><td></td><td></td><td></td><td>Actualización anual Diagnóstico del estado actual del SGSI del INM</td><td></td><td></td><td></td><td>Actualización anual Diagnóstico del estado actual del SGSI del INM</td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">Liderazgo de seguridad de la información</td><td></td><td></td><td colspan="2">Capacitar en seguridad de la información a los roles de seguridad de la información de la empresa.</td><td></td><td></td><td colspan="2">Actividades para madurar los roles de seguridad de la información y su gestión</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td colspan="12">Culturizar a los líderes en su responsabilidad dentro de la seguridad de la información.</td></tr>
<tr><td rowspan="3">Gestión de Riesgos</td><td></td><td colspan="12">Gestión de riesgos y planes de tratamiento de riesgos de seguridad de la información</td></tr>
<tr><td></td><td colspan="4">Uso y apropiación de la gestión de riesgos de seguridad de la información del INM.</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td colspan="2">Automatización de la gestión de riesgos de seguridad de la información.</td><td></td><td></td><td colspan="2">Optimización y maduración de la gestión de riesgos de seguridad de la información</td><td></td><td></td><td colspan="2">Optimización y maduración de la gestión de riesgos de seguridad de la información</td><td></td></tr>
<tr><td>Concientización</td><td></td><td colspan="12">Desarrollo de actividades de uso y apropiación del Modelo de Seguridad y Privacidad de la Información</td></tr>
</table>

Implementación de controles	Implementación de controles de la norma ISO 27001: 2022 y Documentación		Implementar y documentar procedimiento de gestión del cambio de TI	Documentación de políticas de gestión de la configuración, criptografía, devolución y disposición segura de activos de información y gestión de Medios móviles, filtrado URL, sincronización relojes		Documentación de políticas de seguridad para equipos de medición						
			Documentación de políticas de seguridad física	Actualización de Procedimientos y formatos de talento humano, contratos de personal y proveedores		Optimización de seguridad en desarrollo de software						
	DRP		Construcción del DRP	Pruebas de recuperación de escenarios de disrupción			Optimización DRP: Implementación de sitio alterno			Pruebas de recuperación de escenarios de disrupción		
					Evaluación de alternativas para sitio alterno							
	Mantenimiento del SGSI		Validaciones de controles de accesos	Actualización de matriz de activos de información				Actualización de matriz de activos de información			Actualización de matriz de activos de información	
								Auditoría al SGSI	Gestión de los hallazgos de	Actualización de documentos de políticas de seguridad de la información		

									audi toría			
		Remediación de vulnerabilidades			Retest de vulnera bilidade s			Nuevo Análisis de vulnera bilidade s		Remediación de vulnerabilidades		Retest de vulnera bilidade s
		Gestión de los hallazgos de auditoría y calidad que se relacionen con Seguridad y privacidad de la información										
	Mejora miento de la ciberse guridad			Implementació n y gestión de infraestructura de redes, NAC y SIEM	Optimización y gestión de la infraestructura de redes, NAC y SIEM							
				Implementació n de SOC	Gestión de SOC y optimización							
				Implementació n de herramienta gestión de amenazas	Optimización y gestión de inteligencia de amenazas							
			Implem entació n del SGSI en una herram ienta colabor ativa				Optimizar políticas de seguridad en office 365 y nube					
							Implem entació n de herram ienta de borrad o seguro	Implementaci ón de backups fuera de sitio	Implement ación Acceso seguro ZTNA		Implementació n SOAR	
Gestió n de			Desarrollar actividades de uso y apropiación del procedimiento de gestión de incidentes para el personal involucrado y de cómo reportar incidentes para todo el personal									

incidentes de seguridad							Optimización del procedimiento de gestión de incidentes						

8. ANÁLISIS PRESUPUESTAL:

AÑO 2024		AÑO 2025		AÑO 2026	
PROYECTO	**Inversión**	**PROYECTO**	**Inversión**	**PROYECTO**	**Inversión**
Implementación de infraestructura de redes, NAC y SIEM	$1.010.000.000	Optimización DRP	En estudio	Implementación Acceso seguro ZTNA	En estudio
Implementación de SOC		Implementación de backups fuera de sitio	En estudio	Implementación SOAR	En estudio
Implementación de herramienta para inteligencia de amenazas		Implementación de herramienta de borrado seguro	En estudio		
Retest vulnerabilidades	$ 40.000.000	Análisis de vulnerabilidades	$50.000.000	Retest vulnerabilidades	$ 55.000.000
Implementación de control de acceso físico	$ 90.000.000	Optimización DRP	En estudio		
		Implementación de backups fuera INM	En estudio		
Contratista de apoyo para mantener el modelo de seguridad	$ 70.543.000	Contratista de apoyo para mantener el modelo de seguridad	$76.186.440	Contratista de apoyo para mantener el modelo de seguridad	$ 82.281.355

9. RESPONSABLES

CIGD (Comité Institucional de gestión y desempeño): Aprobación del Plan

Jefe OIDT: Garantizar los recursos requeridos y velar por la implementación de plataforma tecnológica del plan

Equipo OIDT: Implementar la plataforma tecnológica que se incluye en el plan

CISO: Velar por la implementación del plan

Responsable de seguridad de la información: Coordinar las actividades de implementación del Plan

10. FICHA DE APROBACION Y CONTROL DE CAMBIOS

Tabla 1. Ficha de aprobación de documentos.

Elaborado por:	**Revisado por:**	**Aprobado por:**
Nombre: Liliana Pineda Aponte **Cargo**: Responsable Seguridad de la información **Fecha**: 2024-04-23	**Nombre**: Rodolfo Gómez **Cargo**: Jefe OIDT **Fecha**: 2024-04-23	Comité Institucional de Gestión y Desempeño/ Acta de aprobación de documentos. **Acta No**. ___ **Fecha**: ____-__-__

Tabla 2. Control de Cambios

FECHA	DESCRIPCIÓN DEL CAMBIO	VERSIÓN
2024-04-23	Creación del documento	1