Plan Estratégico de Seguridad y Privacidad de la Información (PESI)

2024-2026

OIDT

Bogotá, Marzo de 2025

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

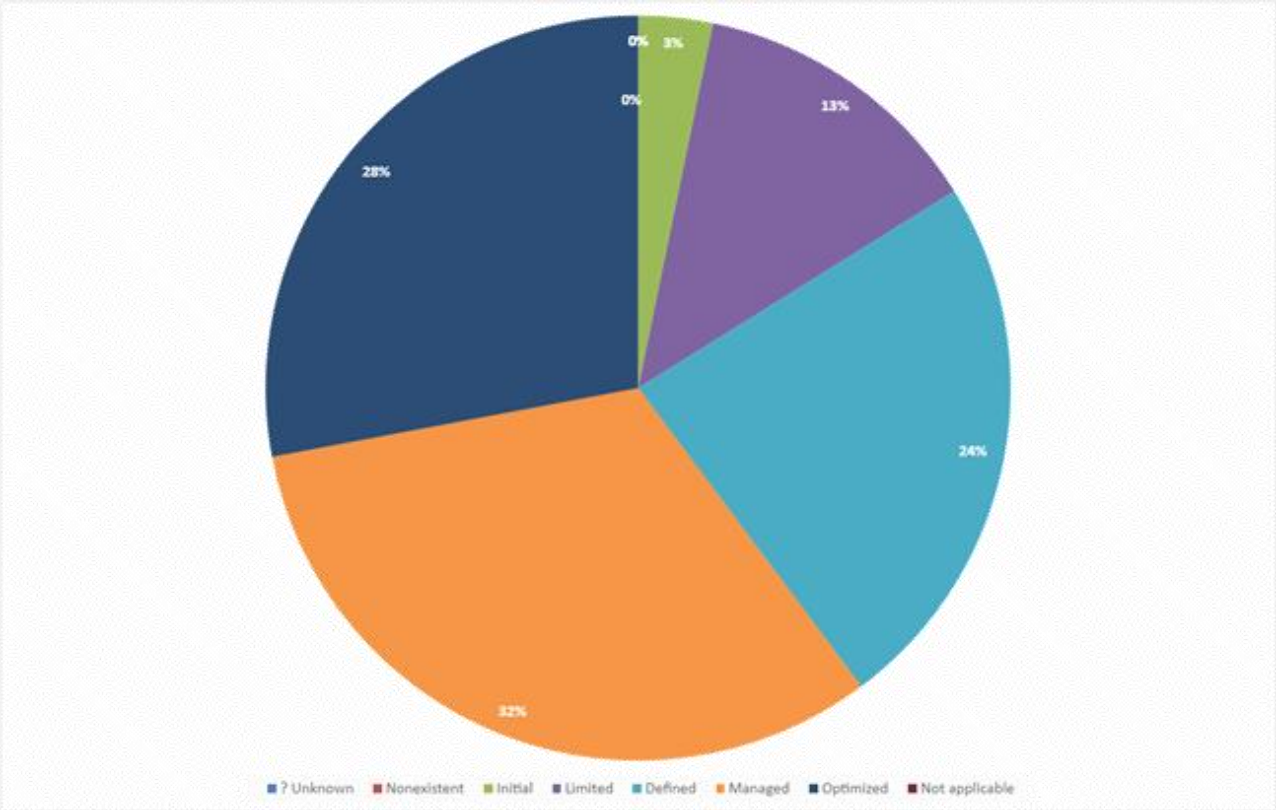
La seguridad y privacidad de la información, es un componente transversal a la Estrategia de Gobierno en línea. Este va alineado con la implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de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

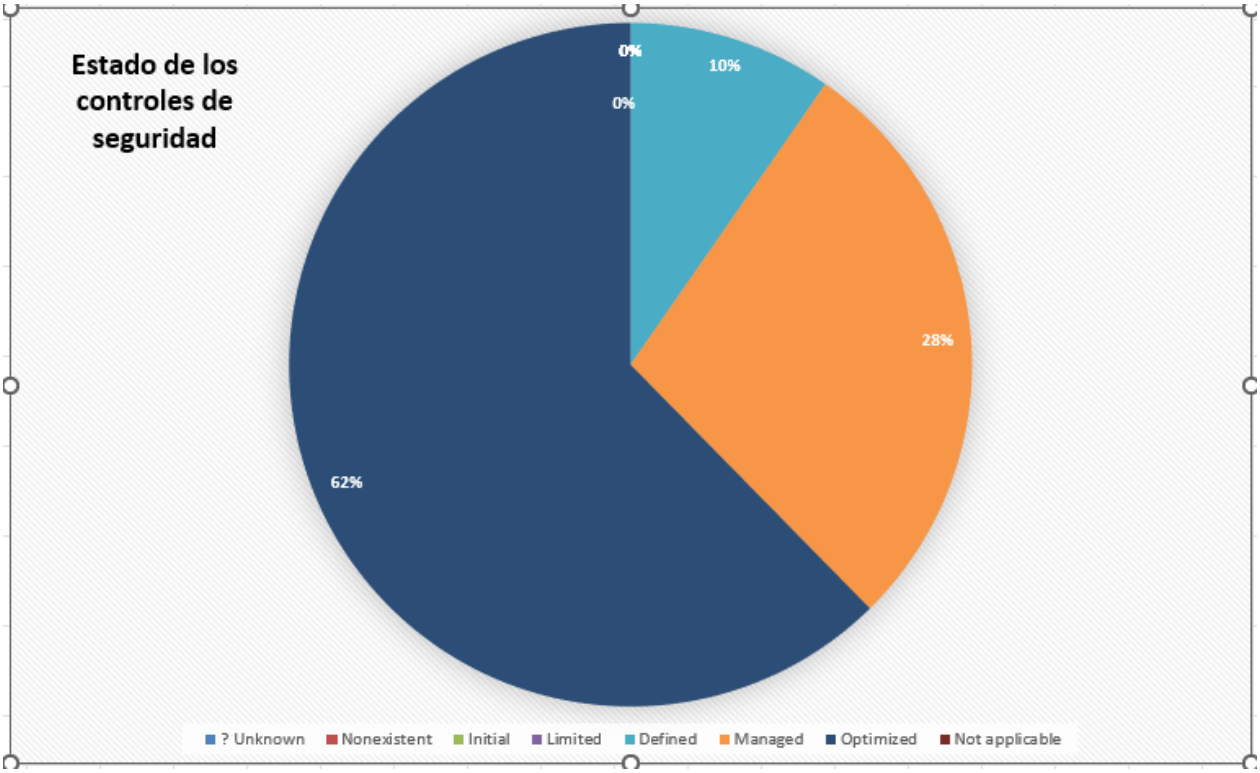
6.1 DIAGNOSTICO DEL ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para establecer el estado actual, el INM ha ejecuta anualmente un diagnóstico del estado de implementación de los controles del anexo A de la norma ISO27001:2022, los cuales se presentan a continuación:

Estado del SGSI basado en el avance de implementación de los controles ISO27001:2022 a diciembre 2023



Estado del SGSI basado en el avance de implementación de los controles ISO27001:2022 a diciembre 2024



Los criterios de medición son los siguientes:

ISO/IEC 27001:2022 ISMS	
Estado	**Criterio**
No Aplica	No aplica.
Inexistente	Falta total de políticas, procedimientos, controles, etc. reconocibles.

Inicial	El desarrollo apenas ha comenzado y requerirá un trabajo significativo para cumplir con los requisitos.
Limitado	Se ha hecho algún progreso, pero aún no se ha completado su implementación
Definido	El control está definido o documentado, aunque faltan detalles y/o aún no se implementa
Administrado	El desarrollo está completo, el proceso/control ha sido implementado, documentado y está operando
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.

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 se ha logrado un avance significativo en la madurez hacia estos niveles óptimos.

El INM hasta el 2023 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:

- 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
- Controles tecnológicos antimalware

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. Actividades para madurar los roles de seguridad de la información y su gestión Culturizar a los líderes en su responsabilidad dentro de la seguridad de la información.	Certificado o evidencia de participación en las capacitaciones Documento de roles y responsabilidades del INM actualizado 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 Uso y apropiación de la gestión de riesgos de seguridad de la información del INM. Automatización de la gestión de riesgos de seguridad de la información. Optimización y maduración de la gestión de riesgos de seguridad de la información	4 Informes de seguimiento a de riesgos de seguridad de la información Piezas comunicativas enviadas por intranet Gestión de riesgos de seguridad en una aplicación de gestión de riesgos Documento con la metodología de riesgos

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
		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.

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Implementación de controles	**Implementación de controles de la norma ISO 27001:2022:** **Elaboración de documentación en el SGSI** Actualización de Políticas y documentos de seguridad de la iformación Establecer lineamientos para la eliminación de información, incluyendo la definición e Implementación de proceso de borrado seguro Gestión de seguridad en plan de gobierno de datos Optimización de seguridad en el desarrollo de software **DRP** **Gestión de ciberseguridad:** Gestión y optimización de infraestructura de redes, NAC y SIEM Gestión y optimización de SOC Gestión y optimización de herramienta de inteligencia de amenazas Optimizar políticas de seguridad en office 365 y nube Revisar viabilidad de Implementación Acceso seguro ZTNA	Manual de políticas, procedimientos, documentos actualizados. Documentos con políticas de seguridad en gestión de TI Herramientas implementadas y documentación elaborada

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
	Análisis y Remediación de vulnerabilidades Actualización de matriz de activos de información **Evaluación el estado de madurez del SGSI**	Documento con las vulnerabilidades y plan de remediación Matriz activos actualizada, aprobada y publicada 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 Optimización del procedimiento de gestión de incidentes	Plan de capacitación y socialización de seguridad y privacidad de la información Evidencias de las capacitaciones en gestión de incidentes Procedimiento de gestión de incidentes actualizado

7. CRONOGRAMA

<table>
<tr><th>ESTRATEGIA DE SEG</th><th>TEMA</th><th colspan="4">AÑO 2025</th><th colspan="4">AÑO 2026</th></tr>
<tr><td></td><td></td><td>TRIMESTRE 1</td><td>TRIMESTRE 2</td><td>TRIMESTRE 3</td><td>TRIMESTRE 4</td><td>TRIMESTRE 1</td><td>TRIMESTRE 2</td><td>TRIMESTRE 3</td><td>TRIMESTRE 4</td></tr>
<tr><td rowspan="2">Liderazgo de seguridad de la información</td><td>Diagnóstico estado seguridad de la información</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></tr>
<tr><td></td><td></td><td></td><td>Planear actividades para madurar los roles de seguridad de la información y su gestión</td><td>Implementar mejoras en los roles de seguridad de la información</td><td colspan="3">Implementar mejoras en los roles de seguridad de la información</td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td>Gestión de riesgos</td><td></td><td></td><td colspan="2">Fortalecimiento de la gestión de riesgos de seguridad de la información</td><td></td><td colspan="2">Fortalecimiento de la Gestión de riesgos de seguridad de la información</td><td></td></tr>
<tr><td>Concientización</td><td></td><td>Establecer plan de capacitación seguridad y Privacidad de la Información</td><td colspan="3">Ejecución del plan de capacitación de seguridad de la información</td><td>Establecer plan de capacitación seguridad y Privacidad de la Información</td><td colspan="3">Ejecución del plan de capacitación de seguridad de la información</td></tr>
<tr><td>Implementación de controles</td><td></td><td></td><td colspan="2">Revisar y actualizar el manual de políticas de seguridad de la información</td><td></td><td colspan="2">Actualización de documentación asociada al SGSI</td><td></td></tr>
</table>

<table>
<tr><td rowspan="13"></td><td rowspan="3"></td><td></td><td>Establecer lineamientos para la eliminación de información, incluyendo la definición e Implementación de proceso de borrado seguro</td><td colspan="2">Gestión de seguridad en plan de gobierno de datos</td><td></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2">Optimización de seguridad en desarrollo de software</td><td></td><td></td><td></td></tr>
<tr><td>DRP</td><td></td><td colspan="2">Pruebas de escenarios DRP y optimización DRP</td><td colspan="3">Pruebas de escenarios de disrupción</td><td></td></tr>
<tr><td rowspan="3"></td><td colspan="2"></td><td></td><td>Actualización de matriz de activos de información</td><td></td><td></td><td>Actualización de matriz de activos de información</td><td></td></tr>
<tr><td></td><td>Análisis de vulnerabilidades</td><td colspan="2">Remediación de vulnerabilidades</td><td colspan="3">Remediación de vulnerabilidades</td><td>Retest de vulnerabilidades</td></tr>
<tr><td colspan="8"></td></tr>
<tr><td rowspan="6">Mejoramiento de la ciberseguridad</td><td colspan="8">Optimización y gestión de la infraestructura de redes y seguridad: NAC y SIEM</td></tr>
<tr><td colspan="8">Gestión de SOC y maduración</td></tr>
<tr><td colspan="8">Optimización y gestión de inteligencia de amenazas</td></tr>
<tr><td></td><td></td><td colspan="2">Optimizar políticas de seguridad en office 365 y nube</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td><td></td><td>Revisar viabilidad de Implementación Acceso seguro ZTNA</td><td></td></tr>
<tr><td></td><td></td><td colspan="2">Planear la implementación de backups fuera de sitio</td><td>Implementar solución backups fuera de sitio</td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">Gestión de incidentes de seguridad</td><td></td><td colspan="8"></td></tr>
<tr><td></td><td></td><td></td><td>Realizar actividad de apropiación de la gestión de incidentes</td><td></td><td></td><td></td><td>Optimización del procedimiento de gestión de incidentes</td><td></td></tr>
</table>

8. ANÁLISIS PRESUPUESTAL:

AÑO 2025		AÑO 2026	
PROYECTO	**Inversión**	**PROYECTO**	**Inversión**
Estudio de solución de backups fuera de sitio	$0	Implementación de backups fuera de sitio	En estudio
Implementación de herramienta de borrado seguro	En estudio		
Soporte NAC, SIEM, inteligencia de amenazas y SOC	$560.000.000		$361.653.710
Análisis de vulnerabilidades	$ 47.400.000	Retest vulnerabilidades	$50.000.000
Contratista de apoyo para mantener el modelo de seguridad	$ 62.312.983	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**: 2025-04-2	**Nombre**: Rodolfo Gómez **Cargo**: Jefe OIDT **Fecha**: 2025-04-2	Comité Institucional de Gestión y Desempeño/ Acta de aprobación de documentos. **Acta No**. ___ **Fecha**: ____-__-__

Tabla 2. Control de Cambios

FECHA	DESCRIPCIÓN DEL CAMBIO	VERSIÓN
2025-04-2	Creación del documento	1