PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CENTRO NACIONAL DE MEMORIA HISTÓRICA

2026-2027

	NOMBRE	CARGO	FECHA
ELABORÓ	Jair Adel Caicedo	Contratistas Gestión de TIC	10/11/2025
REVISÓ	Ronal Alexis Martínez	Profesional especializado Gestión TIC	25/11/2025
REVISÓ	Ana María Trujillo Coronado	Directora Administrativo y Financiero	17/12/2025
APROBÓ	Comité institucional de Gestión y desempeño	Comité institucional de Gestión y desempeño	18/12/2025

TABLA DE CONTENIDO

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la información en la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2026-2027.

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 ejecutar 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.
- Fomentar y consolidar una cultura de seguridad y privacidad de la información en el Centro Nacional de Memoria Histórica (CNMH), orientada al uso responsable, la protección y el manejo adecuado de la información institucional y la memoria histórica que custodia la Entidad.
- Efectuar la detección, análisis y seguimiento de los eventos e incidentes de seguridad de la información, con el propósito de mitigar sus impactos y generar lecciones aprendidas que fortalezcan la gestión y promuevan la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) del Centro Nacional de Memoria Histórica (CNMH).

2. ALCANCE

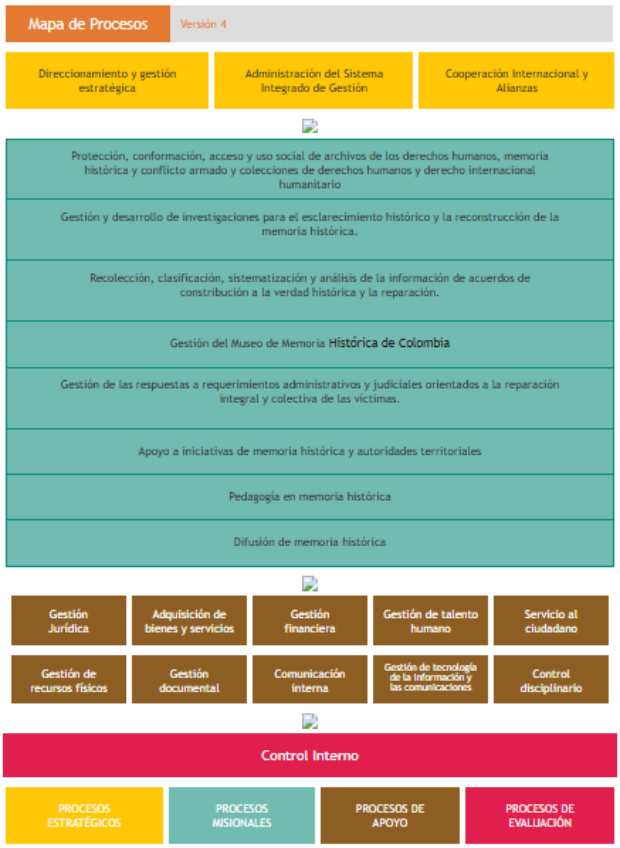
El Plan Estratégico de Seguridad de la Información se posiciona como el marco que impulsa la implementación del Sistema de Gestión de Seguridad de la

Información y la estrategia de seguridad del CNMH. En su esencia, este plan actúa como el enlace primordial entre los diversos componentes de la Política General de Seguridad de la Información, la cual no solo establece lineamientos, sino que también constituye un pilar fundamental en la protección de la integridad, confidencialidad y disponibilidad de la información dentro del CNMH.

En su fundamento, este Plan Estratégico de Seguridad de la Información (PESI) del Centro Nacional de Memoria Histórica (CNMH) se orienta a la identificación, protección y fortalecimiento de los activos de información críticos de la Entidad, mediante la implementación de controles efectivos y la gestión proactiva de los riesgos asociados. Su enfoque integral, preventivo y de mejora continua posiciona al CNMH en un escenario de resiliencia y fortaleza frente a las amenazas emergentes en el entorno digital y a los desafíos propios de la protección de la memoria histórica del país.

este plan no solo busca establecer estándares y protocolos, sino que aspira a crear una cultura organizacional arraigada en la importancia y la responsabilidad compartida en la protección de activos de TI y de la información sensible de la entidad.

En la siguiente ilustración se muestra el mapa de procesos del CNMH que hacen parte del alcance del SGSI:



3. DEFINICIONES

- **Activo:** En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

- **Confidencialidad:** La información no se expone de manera desatendida ni se revela a personas, entidades o procesos no autorizados.

- **Control:** Las directrices, políticas, los procedimientos, las prácticas y las estructuras organizacionales diseñadas para mantener los riesgos de seguridad de la información por debajo del umbral de riesgo aceptado. Control es también un sinónimo de protección o medida preventiva. En términos más sencillos, es una acción que mitiga el riesgo.

- **Disponibilidad:** Garantizar que la información y los sistemas de procesamiento estén accesibles y utilizables por las personas, entidades o procesos autorizados en el momento en que los necesiten.

- **Integridad:** Preservar la precisión y la totalidad de la información, así como de los métodos utilizados para procesarla.

- **Política de Seguridad y Privacidad de la Información:** Declaración explícita de respaldo y compromiso por parte de la alta dirección en relación con la seguridad de la información.

- **Seguridad de la información:** Procesos, procedimientos, controles, guías y medidas preventivas y correctivas que las personas, entidades y las organizaciones adoptan para resguardar y proteger la información y los activos de información, buscando mantener la confidencialidad, disponibilidad e Integridad de los mismos. (ISO/IEC 27000).

- **MSPI:** Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías y Sistemas de Información. Recopilación de mejores prácticas nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo del SGSI, en el marco de la Política de Gobierno Digital, del gobierno nacional.

- **Riesgo:** Probabilidad de que una amenaza específica aproveche una vulnerabilidad, causando pérdida o daño a un activo de información. Esto generalmente se considera como una combinación de la probabilidad de que ocurra un evento y sus consecuencias. (ISO/IEC 27000).

4. DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

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

- Resolución 500 de 2021. "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- NTC/ISO 27001:2013 - NTC/ISO 27001:2022 – NTC/ISO 27005:2009 - GTC/ISO 27002:2015 - GTC/ISO 27002:2022.

5. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El CNMH ha avanzado en la implementación del Modelo de seguridad y privacidad de la información MSPI, establecido por MinTic, a través de los planes que para tal fin se han llevado a cabo en la Entidad en vigencias anteriores, igualmente se han venido realizando ejercicios de medición y diagnostico con el fin de fortalecer el Sistema de Gestión de Seguridad de la Información definido por MINTIC, denominado como Modelo de Seguridad y Privacidad de la Información – MSPI.

RIESGOS CRÍTICOS DE SEGURIDAD.

Riesgos identificados en el proceso de la definición del mapa de riesgos de seguridad, donde se identifica su criticidad según el valor de la evaluación del riesgo.

RIESGO	AMENAZA	EVALUACIÓN	PLAN DE TRATAMIENTO
Pérdida de la Integridad, disponibilidad y confidencialidad de la información.	Daño físico o lógico, parcial o total del Servidor	Alto	El CNMH implementará un plan de tratamiento orientado a mitigar el riesgo de pérdida de integridad, disponibilidad y confidencialidad de la información ante un posible daño físico o lógico de los servidores que respaldan procesos misionales y de apoyo. Para ello, se establecerán acciones preventivas y correctivas que incluyan la aplicación de mantenimientos periódicos, la implementación de mecanismos de redundancia y respaldo automatizado, así como la

RIESGO	AMENAZA	EVALUACIÓN	PLAN DE TRATAMIENTO
			configuración de sistemas de monitoreo y alerta temprana que permitan detectar fallas o accesos no autorizados. Adicionalmente, se fortalecerán los controles de acceso físico al cuarto de servidores y se desarrollará un Plan de Recuperación ante Desastres (DRP) que garantice la restauración oportuna de los servicios en caso de incidentes, asegurando la continuidad operativa y la protección integral de la información institucional.
Pérdida de la Integridad, disponibilidad y confidencialidad de la información	Pérdida total o parcial de la información	Moderado	El CNMH implementará un plan de tratamiento orientado a mitigar el riesgo de pérdida de integridad, disponibilidad y confidencialidad de la información**,** derivado de la ausencia de un proceso formal de copias de seguridad. Se establecerá una política institucional de Backups**,** acompañada de un procedimiento técnico documentado que defina responsabilidades, tipos de respaldo, frecuencia y mecanismos de restauración. Asimismo, se adoptará una herramienta automatizada y segura para la gestión de copias de seguridad, con funciones de cifrado, registro de auditoría y control de acceso, garantizando la trazabilidad de las acciones. El plan contempla la ejecución periódica de pruebas de restauración y la integración de estas actividades al plan de continuidad y recuperación ante desastres (DRP), asegurando la disponibilidad oportuna de la información institucional ante incidentes o fallas tecnológicas.

RIESGO	AMENAZA	EVALUACIÓN	PLAN DE TRATAMIENTO
Pérdida de la Integridad, disponibilidad y confidencialidad de la información	Pérdida total o parcial de la información	Alto	El CNMH implementará un plan de tratamiento enfocado en mitigar el riesgo de divulgación o pérdida de confidencialidad por acceso no autorizado a información pública reservada, fortaleciendo la gestión de accesos, la protección tecnológica y la conciencia del personal. El plan contempla la revisión y actualización de los controles de acceso a sistemas y repositorios que contengan información reservada, definiendo permisos según roles y principios de mínima privilegio. Se implementarán mecanismos de autenticación reforzada (MFA) y registro de auditoría para el seguimiento continuo de accesos. Además, se establecerán copias de seguridad cifradas y un procedimiento para la restauración segura ante incidentes de pérdida o corrupción de datos.

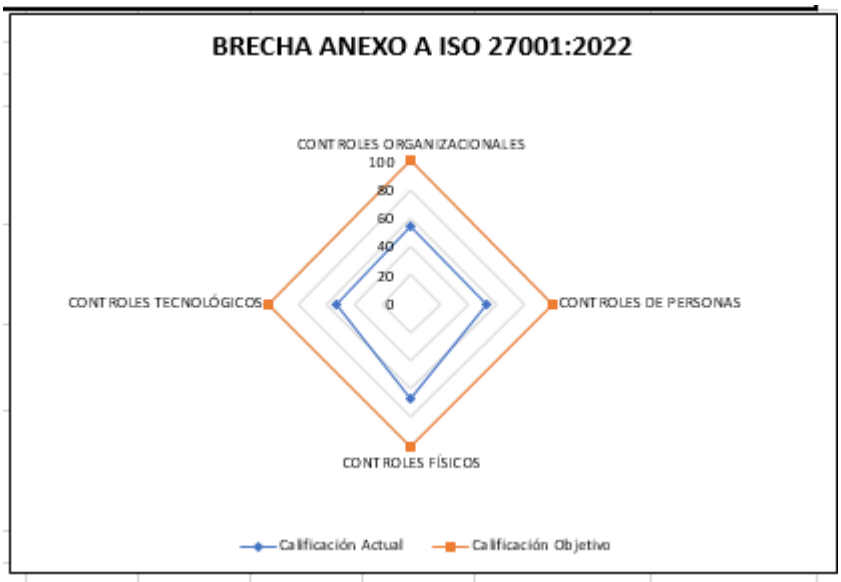
ANÁLISIS DE BRECHAS DE SEGURIDAD, EVALUACIÓN DE CONTROLES Y MEJORA CONTINUA.

El análisis de brechas realizado y la evaluación de controles respecto al Anexo A de la ISO 27001:2022 en el MSPI, ha identificado áreas que requieren atención para mejorar la seguridad de la información. Las brechas destacadas afectan directamente la capacidad de la Entidad para proteger los activos de información y gestionar los riesgos de seguridad. Implementar las recomendaciones obtenidas del autodiagnóstico del MSPI ayudará a cerrar brechas de seguridad, fortalecer la postura de seguridad de la Entidad y cumplir con los requisitos de la ISO 27001:2022.

Se realizará revisión periódica y una mejora continua con el fin de mantener un nivel adecuado de seguridad de la información. A continuación, se presenta el análisis de brechas y evaluación de controles, resultado del autodiagnóstico del MSPI.

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2022 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación	Calificación	Nivel de
A.5	CONTROLES ORGANIZACIONALES	54	100	EFECTIVO
A.6	CONTROLES DE PERSONAS	53	100	EFECTIVO
A.7	CONTROLES FÍSICOS	67	100	GESTIONADO
A.8	CONTROLES TECNOLÓGICOS	53	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		57	100	EFECTIVO



AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

AÑO	COMPONENTE	CLAUSULAS	% de	% Avance Esperado
2025	Planificación	Contexto de la organización	8%	14%
		Liderazgo	7%	14%
		Planificación	7%	14%
		Soporte	8%	14%
	Implementación	Operación	10%	16%
	Evaluación de	Evaluación del desempeño	8%	14%
	Mejora Continua	Mejora	8%	14%
TOTAL			57%	100%

Se presenta el nivel de madurez que se tiene actualmente en la Entidad y sobre el cual se trabaja de manera continua.

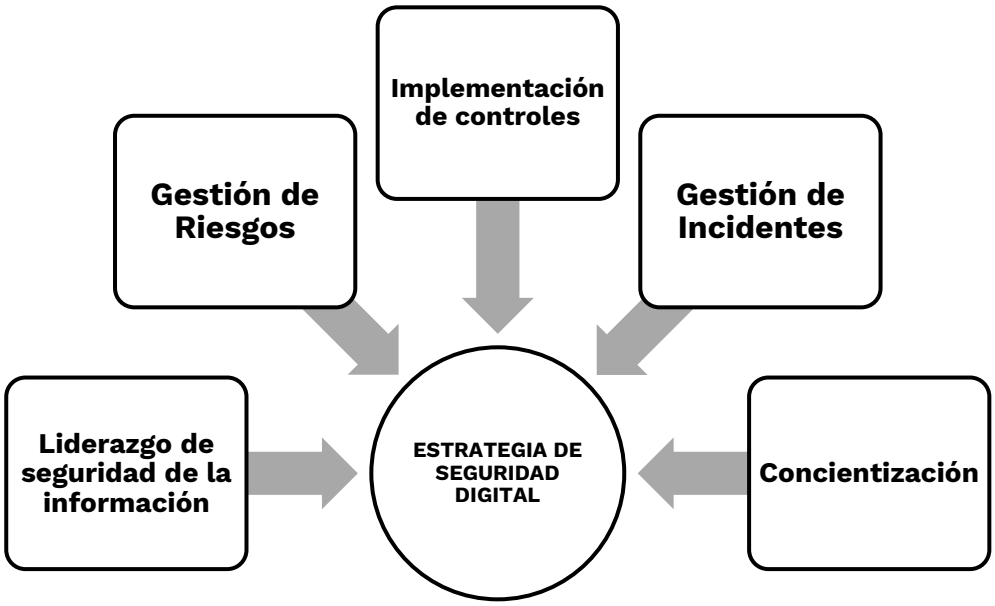
El autodiagnóstico de gobierno digital ha sido un proceso mediante el cual la Entidad ha evaluado su capacidad para implementar y gestionar tecnologías digitales en las operaciones y servicios. Este proceso implica la revisión de varios aspectos de la Entidad incluyendo la infraestructura tecnológica, la gestión de datos, la ciberseguridad, la interoperabilidad de los sistemas, así como la capacitación del personal. Esto ha permitido obtener una visión clara del estado actual sobre la política de gobierno digital y desarrollar un plan estratégico para alcanzar los objetivos de transformación digital.

La medición del FURAG ha Permitido recopilar información sistemática sobre el cumplimiento de los objetivos estratégicos, los planes de acción y los resultados de gestión. A través de esta herramienta, la entidad ha podido evaluar su desempeño en áreas claves como la gestión administrativa, la transparencia, la eficiencia operativa y el cumplimiento normativo.

6. ESTRATEGIA DE SEGURIDAD DIGITAL

La Entidad establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad y privacidad 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 del procedimiento de gestión de incidentes que debe establecerse y debidamente articularse al habilitador de seguridad y privacidad de la Política de Gobierno Digital.

Por tal motivo, **el CNMH** define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



6.1 . DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

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:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad y privacidad 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	Evaluar los riesgos de seguridad de la información mediante una planificación y evaluación detalladas, con el objetivo de prevenir o mitigar los efectos adversos. El elemento central de este proceso es la implementación de controles de seguridad efectivos para gestionar y tratar los riesgos identificados.
Concientización	Fomentar y fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo y apropiando al interior de la entidad 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.

6.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, **el CNMH** define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI). Los proyectos deben estar relacionados tanto con el Manual de políticas como con la política de seguridad definida en la

entidad, además estos proyectos deben corresponder a la implementación de controles que permita mitigar riesgos de seguridad de la información que la entidad haya identificado.

JUSTIFICACIÓN DE LOS PROYECTOS DEFINIDOS

La implementación de los proyectos establecidos en el PESI responde a la necesidad institucional de fortalecer la postura de seguridad y privacidad de la información del CNMH, garantizando el cumplimiento del MSPI, la normatividad vigente (Ley 1581 de 2012, Decreto 103 de 2015, Resolución 500/2021 del MINTIC) y las mejores prácticas internacionales como ISO 27001:2022. Cada proyecto fue definido para cerrar brechas identificadas en el diagnóstico de madurez, mitigar riesgos priorizados, y asegurar que la información histórica, misional y administrativa de la Entidad se gestione con integridad, disponibilidad y confidencialidad en todas sus etapas. Estos proyectos permiten avanzar hacia un modelo de seguridad preventivo, trazable y basado en evidencia, evitando eventos que puedan comprometer la información crítica y la continuidad de las operaciones institucionales.

Estrategias de liderazgo y gobernanza de la seguridad de la información

Los proyectos asociados a este dominio se justifican en la necesidad de consolidar una estructura de liderazgo formal que permita planear, dirigir y supervisar la seguridad de la información desde un enfoque estratégico. La actualización de políticas institucionales y la definición de roles y responsabilidades generan un marco claro para la toma de decisiones, la asignación de recursos y la articulación entre áreas. Sin un liderazgo formal y visible, las actividades de seguridad terminan dispersas, reactivas y sin soporte directivo, lo que aumenta la exposición a incidentes y reduce la eficacia del MSPI. Estos proyectos permiten institucionalizar la seguridad de la información como un componente transversal y misional del CNMH.

Proyectos de Gestión de Riesgos

La justificación de estos proyectos radica en la necesidad de establecer un proceso sistemático, medible y permanente para identificar, analizar,

valorar y tratar los riesgos que afectan los activos de información del CNMH. Dada la naturaleza sensible de la información administrada incluyendo datos personales, información pública clasificada, repositorios históricos y evidencia documental, un enfoque de gestión de riesgos permite anticipar amenazas, reducir vulnerabilidades y priorizar la asignación de recursos. Estos proyectos garantizan que la Entidad gestione su información con criterios técnicos y con la capacidad de prevención necesaria para proteger su misión institucional.

Proyectos de Concientización y Cultura de Seguridad

La mayoría de incidentes y brechas se derivan de errores humanos, desconocimiento o malas prácticas en el manejo de la información. La cultura organizacional es un pilar del MSPI, y fortalecerla permite reducir significativamente la probabilidad de fugas de información, accesos indebidos, manipulaciones incorrectas de datos o incumplimientos normativos. La formación continua del personal aumenta la capacidad de detección temprana de incidentes, facilita el cumplimiento de políticas y empodera a los funcionarios para proteger los activos de información en su quehacer diario. Estos proyectos contribuyen directamente a disminuir riesgos de tipo humano-operativo y fortalecen la corresponsabilidad institucional.

Implementación y Fortalecimiento de Controles.

Se plantea la necesidad de establecer controles técnicos, administrativos y físicos que permitan fortalecer la protección de la información frente a amenazas internas y externas. La implementación de controles es fundamental para cumplir con el Anexo A de ISO 27001:2022 y con los dominios del MSPI (organizacionales, personas, físicos y tecnológicos). Al definir controles de seguridad, se garantiza que la infraestructura del CNMH opere con niveles adecuados de seguridad, estabilidad y continuidad. Con lo anterior se reducen brechas identificadas en el autodiagnóstico del MSPI y mitigan riesgos prioritarios que afectan la disponibilidad de los servicios institucionales.

Proyectos de Gestión de Incidentes.

Estos se basan en la urgencia de contar con mecanismos formales, estructurados y automatizados para prevenir, detectar, contener y responder a incidentes de seguridad de la información. Actualmente, el incremento de amenazas cibernéticas y la dependencia de tecnologías digitales exige que la Entidad cuente con procedimientos estandarizados, roles claros, herramientas tecnológicas y tiempos de respuesta eficientes. Estos proyectos permiten asegurar la continuidad operativa, minimizar el impacto de incidentes y fortalecer la capacidad institucional para generar evidencia, reportar, escalar y mejorar continuamente el proceso. Además, responden a los lineamientos del MINTIC sobre la Gestión de Incidentes y a los requisitos del MSPI para mantener trazabilidad, auditoría y respuesta efectiva.

A continuación, se relacionan los proyectos dimensionados para el robustecimiento de la postura de Seguridad de la información de la Entidad.

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	**PROYECTO 1:** Actualiza, Desarrollar e implementar una política de seguridad y privacidad de la información **PROYECTO 2:** Definición de Roles y Responsabilidades de Seguridad de la Información. **PROYECTO 3** Actualizar los controles de seguridad de la Versión 27001:2013 a la Versión 27001:2022	**PROY.1.** actualizar la política de seguridad de la información y aumentar la madurez del Modelo de Seguridad y Privacidad de la Información (MSPI). Revisión y verificación de Roles y Responsabilidades. **PROY.2.** Definición de los Roles y Responsabilidades en Seguridad de la Información formalizados dentro de las políticas de seguridad. **PROY.3.** Declaración de aplicabilidad ISO27001:2022 y

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
		desarrollo del MSPI ISO27001:2022
Gestión de riesgos	**PROYECTO 1:** Identificar, valorar y clasificar los riesgos asociados a los activos de información. **PROYECTO 2:** Definir planes de tratamiento de riesgos de seguridad. **PROYECTO 3:** Fortalecer e Implementar una solución de respaldo para copias de seguridad de la información lo cual permitirá el fortalecimiento de los procesos de Backup y aseguramiento de la información de la Entidad.	**PROY.1.** Matriz de riesgos de seguridad digital **PROY.2**. Definir planes de tratamiento de riesgos. **PROY.3.** Implementación de la adquisición y/o contratación de una estrategia automatizada para copias de seguridad.
Concientización	**PROYECTO 1:** Establecer desde el inicio de cada año la planeación de sensibilización para todo el año sobre SPI. **PROYECTO 2:** Realizar jornadas de sensibilización y/o comunicación de seguridad de la información a todo el personal de la Entidad. **PROYECTO 3:** Medir el grado de sensibilización a toda la Entidad.	**PROY.1.** plan de apropiación y sensibilización de SPI. **PROY.2.** Evidencias de las actividades desarrolladas. **PROY.3.** Resultado de las encuestas de medición

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Implementación de controles	**CONTROL 1** Fortalecimiento de la Política de las copias de seguridad de la información. **CONTROL 2** Clasificación de la información (Publica, Publica clasificada, Publica reservada). **CONTROL 3** Implementación de doble factor de autenticación. **CONTROL 4** Políticas de Desarrollo Seguro. **CONTROL 5** Control de acceso físico Centro de datos.	1. Política de respaldos de información. 2. Clasificación de la información. 3. Implementación de doble factor de autenticación. 4. Políticas de Desarrollo Seguro. 5. Controles de acceso a áreas protegidas o áreas seguras.
Gestión de incidentes	**PROYECTO 1:** Revisión de seguimiento y mejoramiento del procedimiento de Gestión de Incidentes. **PROYECTO 2:** Capacitar al personal en la gestión de incidentes de seguridad de la información. **PROYECTO 3:** Llevar a cabo la implementación de un Correlacionador de eventos que orqueste todos los eventos de seguridad y permita tomar acciones preventivas y correctivas de SPI. **PROYECTO 4:** Llevar a cabo la implementación de un SOC (Security Operations Center),	1. Procedimiento de gestión de incidentes de seguridad formalizado. 2. Sesiones de capacitación desarrolladas. 3. Implementación de un Correlacionador.

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
	garantiza una supervisión constante de la red, servidores, servicios y aplicaciones institucionales y permite detectar, analizar y responder en tiempo real a incidentes de seguridad, lo que mejora la capacidad del CNMH para proteger la información sensible, los datos personales y los activos críticos.	

6.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

Dando alcance a los proyectos y/o actividades descritas anteriormente se establece el cronograma a tener en cuenta para el desarrollo de las actividades.

AÑO 2025				AÑO 2026				AÑO 2027			
TRIMES1	**TRIMES2**	**TRIMES3**	**TRIMES4**	**TRIMES1**	**TRIMES2**	**TRIMES3**	**TRIMES4**	**TRIMES1**	**TRIMES2**	**TRIMES3**	**TRIMES4**
		Actualiza, Desarrollar e implementar una política de seguridad y privacidad de la información.		Fortalecer e Implementar una solución de respaldo para copias de seguridad de la información lo cual permitirá el fortalecimiento de los procesos de Backup y aseguramiento de la información de la Entidad.				Llevar a cabo la implementación de un Correlacionador de eventos que orqueste todos los eventos de seguridad y permita tomar acciones preventivas y correctivas de SPI.			
		Definición de Roles y Responsabilidades de Seguridad de la Información.			Actualiza, Desarrollar e implementar una política de seguridad y privacidad de la información.				Actualiza, Desarrollar e implementar una política de seguridad y privacidad de la información.		
		Actualizar los controles de seguridad de la Versión 27001:2013 a la Versión 27001:2022		Establecer desde el inicio de cada año la planeación de sensibilización para todo el año sobre SPI.	Realizar jornadas de sensibilización y/o comunicación de seguridad de la información a todo el personal de la Entidad.			Llevar a cabo la implementación de un SOC (Security Operations Center), garantiza una supervisión constante de la red, servidores, servicios y aplicaciones institucionales y permite detectar, analizar y responder en tiempo real a incidentes de seguridad, lo que mejora la capacidad del CNMH para proteger la información sensible, los datos personales y los activos críticos.			
		Identificar, valorar y clasificar los riesgos asociados a los activos de información.				Medir el grado de sensibilización a toda la Entidad.		Establecer desde el inicio de cada año la planeación de sensibilización para todo el año sobre SPI.	Realizar jornadas de sensibilización y/o comunicación de seguridad de la información a todo el personal de la Entidad.		
		Definir planes de		Implementación y seguimiento de Controles				Implementación y seguimiento de Controles			

AÑO 2025				AÑO 2026				AÑO 2027			
TRIMES1	**TRIMES2**	**TRIMES3**	**TRIMES4**	**TRIMES1**	**TRIMES2**	**TRIMES3**	**TRIMES4**	**TRIMES1**	**TRIMES2**	**TRIMES3**	**TRIMES4**
		tratamiento de riesgos de seguridad.									
					Revisión de seguimiento y mejoramiento del procedimiento de Gestión de Incidentes.	Capacitar al personal en la gestión de incidentes de seguridad de la información.				Medir el grado de sensibilización a toda la Entidad.	

Nota: Al finalizar cada vigencia, LA ENTIDAD, realizará una actualización del cronograma, incorporando el estado del avance de los proyectos formulados y si en efecto se cumplieron o se plantean aplazamientos para las vigencias posteriores. Así mismo, el cronograma podrá ser modificado o ajustado de acuerdo con las necesidades o situaciones que surjan en la entidad.

6.4 ANÁLISIS PRESUPUESTAL:

Con base a los proyectos definidos y su proyección, el presupuesto de este plan está incluido en el PETI 2026-2027.

7. RESPONSABLES

1. Dirección Administrativa y Financiera: Aprobar los documentos de Alto Nivel
2. Gestión de Tecnologías de la Información (Gestión TIC): Velar por la implementación del MSPI y garantizar los recursos requeridos.
3. Responsables de Seguridad Digital: Coordinar las actividades de implementación del MSPI

8. APROBACIÓN

El presente plan fue sometido a consideración y conocimiento de la Alta Dirección y del Comité Institucional de Gestión y Desempeño, en sesión realizada el 18 de diciembre de 2025, según consta en el Acta de aprobación No. 15 de 2025, con el fin de ser aprobado y aplicado conforme a los lineamientos y disposiciones aquí establecidos.