PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

CENTRO NACIONAL DE MEMORIA HISTÓRICA

2026-2027

	NOMBRE	CARGO	FECHA
ELABORÓ	Angelica María Angel Jair Adel Caicedo	Contratistas Gestión de TIC	10/11/2025
REVISÓ	Fabio Velandia Quecan	Profesional especializado Gestión TIC	30/11/2025
REVISÓ	Ronal Alexis Martínez	Profesional especializado Gestión TIC	30/11/2025
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 DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

1. INTRODUCCIÓN

La información es uno de los activos más valiosos del Centro Nacional de Memoria Histórica (CNMH), y su adecuada gestión es esencial para garantizar la confianza institucional, la transparencia pública y la continuidad de las operaciones.

El presente Plan de Seguridad y Privacidad de la Información 2026–2027 establece las acciones estratégicas, técnicas y organizacionales que orientan la protección de los activos de información frente a amenazas, vulnerabilidades y riesgos que puedan afectar su confidencialidad, integridad y disponibilidad.

El plan se enmarca en los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Gobierno Digital, la ISO/IEC 27001:2022, y la Guía DAFP V.7 (2025) de gestión integral del riesgo.

2. OBJETIVO

Fortalecer la gestión de la seguridad y privacidad de la información en el CNMH mediante actividades que permitan establecer, operar, monitorear, revisar y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información – MSPI y seguridad digital.

2.1 Objetivos específicos

- Implementar y mantener el Sistema de Gestión de Seguridad de la Información (SGSI) alineado al MSPI.
- Promover la cultura institucional de seguridad digital entre funcionarios, contratistas y terceros del CNMH.

3. ALCANCE

Este plan aplica a todos los procesos, funcionarios, contratistas y terceros del Centro Nacional de Memoria Histórica (CNMH) que acceden, usan o gestionan información institucional.
Cubre todos los activos de información, sin importar su formato o ubicación, así como los sistemas, servicios y plataformas tecnológicas que los soportan.
Su propósito es fortalecer la gestión de la seguridad y privacidad de la información mediante la implementación, operación y mejora continua del

Modelo de Seguridad y Privacidad de la Información (MSPI) y del Sistema de Gestión de Seguridad de la Información (SGSI) en el CNMH.

4. DEFINICIONES

Activo: Cualquier elemento que tiene valor para la organización y que para la Gestión de riesgos de seguridad de la información se consideran los siguientes entre otros como la información, el software, los elementos físicos, los servicios, las personas e intangibles.

Activo de información: Cualquier cosa que tenga valor para la organización y que contribuya al logro de sus objetivos, incluyendo la información, los medios que la procesan, almacenan o transmiten, y los recursos humanos que la gestionan. [Fuente: ISO 27000]

Amenaza: Causa potencial de un incidente no deseado, el cual puede resultar en daño al sistema o a la Organización. [Fuente: ISO 27000]

Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento**.**

Confidencialidad: Propiedad de la información que hace que no esté disponible o que no pueda ser revelada a individuos, entidades o procesos, no autorizados.

CSIRT: Equipo de respuesta a incidentes cibernéticos del país

Control: Acción, medida o mecanismo implementado con el propósito de modificar un riesgo, sea para prevenir su ocurrencia o reducir sus efectos adversos."
"Los controles pueden ser manuales o automáticos, y deben asociarse a responsables, periodicidad de aplicación y mecanismos de verificación. [Fuente: GUIA PARA LA GESTION INTEGRAL DEL RIESGOS V7 DAFP 2025]

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581/2012).

Disponibilidad: Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada. [Fuente: ISO 27000]

Importancia del activo: Valor que refleja el nivel de protección requerido por un activo de información frente a las tres propiedades de la seguridad de la información: integridad, confidencialidad y disponibilidad.

Integridad: Propiedad de precisión y completitud. [Fuente: ISO 27000]

Monitoreo: Verificación, supervisión, observación crítica o determinación continua del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

MSPI: Modelo de Seguridad y Privacidad de la Información.

Parte involucrada: Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o una actividad. Una persona que toma decisiones puede ser una parte involucrada. [Fuente: ISO 31000]

Propietario del activo: Persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El propietario del activo aprueba el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.

Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización). [Fuente: ISO 31000]

Seguridad de la Información: Conjunto de medidas técnicas, humanas, físicas y administrativas adoptadas por las entidades públicas para proteger los activos de información y garantizar su confidencialidad, integridad y disponibilidad. [Fuente: MSPI]

Sensibilización: Proceso mediante el cual se comunica y promueve la comprensión de la importancia de la seguridad de la información y del cumplimiento de las políticas, procedimientos y controles establecidos en la organización. [Fuente: ISO 27000]

SGSI: Sistema de Gestión de Seguridad de la Información

Teletrabajo: En Colombia, el Teletrabajo se encuentra definido en la Ley 1221 de 2008 como: "*Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación -TIC- para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio especifico de trabajo*". (Artículo 2, Ley 1221 de 2008)

Vulnerabilidad: Debilidad identificada sobre un activo y que puede ser aprovechada por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.

5. MARCO LEGAL

Ley 1581 de 2012 – Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamenta los principios, derechos y procedimientos aplicables al tratamiento de datos personales, y define las obligaciones de las entidades públicas y privadas en materia de seguridad, confidencialidad y autorización del titular.

Decreto 1377 de 2013 – Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Establece las disposiciones para la implementación de políticas de tratamiento de datos personales, los mecanismos de autorización y los procedimientos de actualización, rectificación y supresión de datos.

Ley 1712 de 2014 – Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Garantiza el derecho de acceso a la información pública y promueve la transparencia activa, la protección de datos personales y el equilibrio entre el principio de publicidad y la reserva legal.

Decreto 103 de 2015 – Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Regula los procedimientos y estándares para la publicación, accesibilidad, gestión y clasificación de la información pública.

Conpes 3854 de 2016 – Por el cual se adopta la Política Nacional de Seguridad Digital. Define los lineamientos estratégicos para fortalecer las capacidades nacionales de gestión, mitigación y respuesta ante riesgos y amenazas en el entorno digital, promoviendo la cooperación y la corresponsabilidad entre los sectores público y privado.

Resolución 2140 de 2017 – Por la cual se adopta el Modelo Integrado de Planeación y Gestión (MIPG). Establece el marco de articulación de las políticas de gestión y desempeño institucional, incluyendo la gestión de riesgos, la transparencia y la seguridad de la información.

Resolución 1519 de 2020 – Por la cual se definen los estándares y directrices para la publicación de información señalada en la Ley 1712 de 2014. Determina los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital y datos abiertos, en concordancia con la Política de Gobierno Digital.

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 de la Información como habilitador de la Política de Gobierno Digital. Fija los criterios técnicos y organizacionales para la implementación del modelo, en coherencia con los principios de la Política de Gobierno Digital.

Directiva Presidencial 02 de 2022 – Por la cual se imparten lineamientos para garantizar la implementación segura de la Política de Gobierno Digital liderada por el MinTIC. Ordena a las entidades públicas adoptar

medidas de fortalecimiento en materia de ciberseguridad, gestión del riesgo digital y protección de la información.

Decreto 338 de 2022 – Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital. Crea el Modelo de Gobernanza de la Seguridad Digital y las instancias responsables de su implementación en el Estado colombiano.

Resolución 746 de 2022 – Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021. Define roles, responsabilidades, controles y mecanismos de monitoreo para la gestión integral de la seguridad y la privacidad en las entidades públicas.

Decreto 767 de 2022 – Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital. Subroga el Capítulo 1 del Título 9 del Decreto 1078 de 2015 e integra la gestión de información, servicios ciudadanos digitales, seguridad y datos abiertos como habilitadores de la transformación digital del Estado.

Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (DAFP, 2025) – Por la cual se actualizan los lineamientos para la identificación, valoración y tratamiento de riesgos. Incorpora el enfoque integral de riesgo aplicable a los ámbitos de gestión, corrupción y seguridad digital, alineado con los estándares internacionales ISO 31000 e ISO/IEC 27005.

ISO/IEC 27001:2022 – Por la cual se establecen los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Define las buenas prácticas internacionales para proteger la información y gestionar los riesgos asociados.

6. METODOLOGÍA

La metodología propuesta para la creación del Plan de seguridad de la información ese define en las siguientes etapas:

- Etapa 1: Conocer la entidad.
- Etapa 2: Diagnóstico inicial.
- Etapa 3: Generación del plan.
- Etapa 4: Mejora continua

Ilustración 1 Ciclo del Modelo de Seguridad y Privacidad de la Información FUENTE: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401770_recurso_1.pdf

6.1. ETAPA 1: CONOCER LA ENTIDAD

El Centro Nacional de Memoria Histórica (CNMH) adopta e implementa el Modelo de Seguridad y Privacidad de la Información (MSPI), elaborado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), como marco de referencia para la gestión integral de la seguridad y privacidad de los activos de información institucional.
Este modelo define los lineamientos para la implementación de la estrategia de seguridad digital en las entidades públicas, con el propósito de formalizar un Sistema de Gestión de Seguridad de la Información (SGSI) y fortalecer la seguridad digital institucional, en concordancia con los requerimientos legales, técnicos, normativos y reglamentarios vigentes.

El SGSI del CNMH se estructura bajo el enfoque del ciclo de mejoramiento continuo PHVA (Planear, Hacer, Verificar y Actuar), asegurando la planeación, ejecución, evaluación y mejora constante de las acciones orientadas a la protección de la información. Este modelo integra cinco (5) fases, que permiten gestionar y mantener adecuadamente la seguridad y privacidad de la información en todos los procesos, trámites, servicios, sistemas de información, infraestructura tecnológica y, en general, en los activos de información que custodia la entidad.

A continuación, se presentan las fases implementadas en el CNMH conforme al MSPI:

Fase 1. Diagnóstico. Corresponde a la evaluación del estado actual de la seguridad y privacidad de la información en el CNMH, mediante la aplicación del instrumento de evaluación del MSPI del MinTIC. Esta fase permite identificar los activos críticos de información, analizar los riesgos, determinar brechas de cumplimiento y valorar el nivel de madurez institucional frente a los controles definidos en la norma ISO/IEC 27001:2022 y el MSPI.

Fase 2. Planificación. Consiste en determinar los objetivos, estrategias y necesidades de seguridad y privacidad de la información, considerando el contexto institucional, el mapa de procesos y las prioridades misionales.
Durante esta fase se elabora el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se actualizan las políticas y se establecen los controles y responsables de su implementación.

Fase 3. Operación. Incluye la ejecución de las estrategias, controles y medidas definidas en el plan de seguridad.
En esta fase, el CNMH desarrolla actividades de fortalecimiento técnico, administrativo y de talento humano, mediante la adopción de mecanismos de protección, herramientas tecnológicas y programas de sensibilización en seguridad digital.

Fase 4. Evaluación del desempeño. Comprende el seguimiento y la verificación del desempeño del SGSI mediante la revisión de indicadores, auditorías internas y análisis de eficacia de los controles implementados. Esta fase permite garantizar la trazabilidad de las acciones, medir el cumplimiento de los objetivos establecidos y promover la mejora continua del sistema.

Fase 5. Mejoramiento continuo. Implica el establecimiento de procedimientos para identificar desviaciones, no conformidades o brechas detectadas en las fases anteriores, definiendo las acciones correctivas y preventivas necesarias para su solución y no repetición.

El CNMH mantiene mecanismos de revisión y actualización del modelo, asegurando su alineación con las nuevas disposiciones normativas y los requerimientos del MinTIC.

En cumplimiento de lo anterior, el CNMH establece, actualiza, aprueba y divulga los documentos estratégicos asociados al MSPI y al SGSI, tales como:

- La Política de Seguridad y Privacidad de la Información,
- El Plan de Seguridad y Privacidad de la Información,
- El Plan de Tratamiento de Riesgos de Seguridad y Privacidad
- y la documentación asociada al autodiagnóstico del MSPI.

Estos instrumentos permiten definir y ejecutar las estrategias, controles y acciones necesarias para proteger la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional, mitigar los riesgos asociados, garantizar la continuidad operativa y asegurar el cumplimiento de los lineamientos establecidos por el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Política de Gobierno Digital.

6.2. ETAPA 2: DIAGNOSTICO

Consiste en la realización del análisis de brechas, frente a la norma la ISO 27001: 2022. Para este caso, el análisis se realizará mediante el uso del "Instrumento de evaluación MSPI", de MinTIC. Este instrumento no solo evalúa los requerimientos solicitados MinTIC y los de la norma ISO 27001: 2022. Adicionalmente evalúa ciberseguridad y el ciclo PHVA. A continuación, se muestra el resultado de la implementación de los controles evaluados e el MSPI 2025:

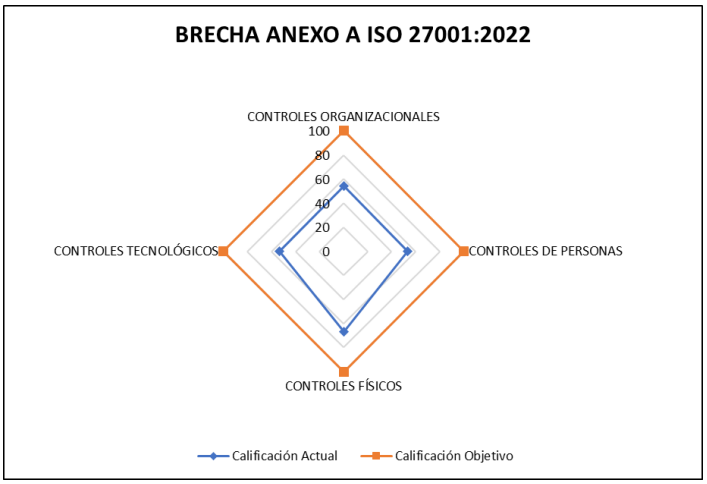

Ilustración 2 Brechas MSPI-2025

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

Tabla 1 Evaluación de los controles

6.3. ETAPA 3: GENERACION DEL PLAN

Con base en la información anteriormente recopilada en las fases anteriores se genera el Plan de seguridad y Privacidad de la Información para la vigencia 2026 -2027 del CNMH, se centra en el análisis, ejecución y cumplimiento de las actividades y objetivos planeados, teniendo en cuenta los roles y responsabilidades y los tiempos de cumplimiento por parte del equipo de trabajo involucrado (todos los procesos, actores clave, colaboradores, equipo directivo, partes interesadas, entre otros). El resultado esperado de esta fase es la adecuada implementación y cumplimiento de las actividades previstas en el presente documento.

COMPONENTE	ACTIVIDAD	TAREA	EVIDENCIA	RESPONSABLE	DURACION (MES)	
					Inicio	fin
Activos de Información	Actualización activos de información.	Gestionar el proceso de actualización de los activos de información con los procesos del CNMH.	Activos de información actualizados en el formato institucional.	Procesos Gestión TIC	Cuando se requiera	Cuando se requiera
	Consolidación de los activos de información de las dependencias.	Consolidar los activos de información de las dependencias.	Registro de activos de información	Gestión TIC	Cuando se requiera	Cuando se requiera

COMPONENTE	ACTIVIDAD	TAREA	EVIDENCIA	RESPONSABLE	DURACION (MES)	
					Inicio	fin
	Aprobación activos de información.	Socializar ante el CIGD para aprobación los activos de información	Acta del comité o Presentación (ppt) de temas al comité en dónde fue aprobado.	Gestión TIC	Cuando se requiera	Cuando se requiera
	Publicación del registro de activos de información.	Publicar en la página web, el registro de activos de información.	URL de publicación.	Gestión TIC	Cuando se requiera	Cuando se requiera
Gestión de Riesgos de Seguridad de la Información	Actualización riesgos de seguridad de la Información.	Gestionar el proceso de actualización de los riesgos de seguridad de la información a partir de los activos de información de los procesos del CNMH.	Mapa de riesgos de SI actualizados.	Procesos-Gestión TIC	Cuando se requiera	Cuando se requiera
	Consolidación de los riesgos de seguridad de la información de los procesos.	Consolidar los riesgos de seguridad de la información dependencias.	Mapa de riesgos consolidados.	Gestión TIC	Cuando se requiera	Cuando se requiera
	Aprobación Riesgos de SI	Gestionar la aprobación de los riesgos de SI	Acta del comité o Presentación (ppt) de temas al comité en dónde fue aprobado.	Gestión TIC	Cuando se requiera	Cuando se requiera
Gestión de Incidentes de Seguridad de la Información	Incidentes de Seguridad de la Información gestionados	Gestionar los incidentes de seguridad de la información reportados a la mesa de asistencia.	Casos de soporte gestionados de los incidentes de SI	Gestión TIC	Cuando se requiera	Cuando se requiera
Documentación SGSI	Formulación y/o actualización de la documentación del SGSI	Formular y/o actualizar la documentación de seguridad de la información.	Documentación publicada en la intranet y/o página web de la entidad.	Gestión TIC	Cuando se requiera	Cuando se requiera

COMPONENTE	ACTIVIDAD	TAREA	EVIDENCIA	RESPONSABLE	DURACION (MES)	
					Inicio	fin
Diagnostico MSPI	Aplicación del instrumento de diagnóstico MSPI	Aplicar el instrumento diagnostico MSPI	Matriz MSPI	Gestión TIC	Cuando se requiera	Cuando se requiera
	Planteamiento para el cierre de brechas identificadas en instrumentos MSPI	Aplicar el instrumento diagnostico MSPI	Estrategia para el cierre de brechas	Gestión TIC	Cuando se requiera	Cuando se requiera
Plan de Tratamiento de Riesgos	Revisión y actualización del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Revisar y actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.		Gestión TIC	Cuando se requiera	Cuando se requiera
	Aprobación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Socializar ante el CIGD el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Acta del comité o Presentación (ppt) de temas al comité en dónde fue aprobado.	Gestión TIC	Cuando se requiera	Cuando se requiera
	Publicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Publicar en la página web, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Link página web	Gestión TIC	Cuando se requiera	Cuando se requiera
Plan de Seguridad y Privacidad de la Información	Revisión y actualización del Plan de Seguridad y Privacidad de la Información	Revisar y actualizar el Plan de Seguridad y Privacidad de la Información		Gestión TIC	Cuando se requiera	Cuando se requiera
	Aprobación del Plan de Seguridad y Privacidad de la Información	Socializar ante el CIGD el Plan de Plan de Seguridad y Privacidad de la Información	Acta del comité o Presentación (ppt) de temas al comité en dónde fue aprobado.	Gestión TIC	Cuando se requiera	Cuando se requiera

COMPONENTE	ACTIVIDAD	TAREA	EVIDENCIA	RESPONSABLE	DURACION (MES)	
					Inicio	fin
	Publicación del Plan de Seguridad y Privacidad de la Información	Publicar en la página web, el Plan de Seguridad y Privacidad de la Información	Link página web	Gestión TIC	Cuando se requiera	Cuando se requiera
Sensibilización en seguridad de la información.	Campañas y jornadas de sensibilización en seguridad digital	Sensibilizar al personal sobre el SGSI	Actas de participación, registros de asistencia y materiales divulgativo	Gestión TIC	Cuando se requiera	Cuando se requiera
Proveedores TIC	Evaluación de proveedores y servicios tecnológicos	Verificar cumplimiento de cláusulas de seguridad digital en contratos	Informe de evaluación y seguimiento contractual	Gestión TIC	Cuando se requiera	Cuando se requiera

6.4. ETAPA 4: MEJORA CONTINUA

El proceso de mejora continua del Plan de Seguridad y Privacidad de la Información del CNMH se fundamenta en el ciclo de gestión PHVA (Planear, Hacer, Verificar y Actuar) establecido en el Modelo de Seguridad y Privacidad de la Información MSPI y la norma ISO/IEC 27001:2022.

Las actividades descritas en el numeral 6.3 "Generación del Plan" constituyen la base operativa para la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), ya que permiten mantener actualizados los activos de información, los riesgos, los planes de tratamiento, los instrumentos estratégicos y los mecanismos de sensibilización institucional.

De manera transversal, la mejora continua se materializa en la revisión periódica del desempeño del SGSI, la actualización de documentos estratégicos, la atención a hallazgos de auditoría, la evaluación de proveedores tecnológicos, la aplicación anual del diagnóstico MSPI y la ejecución de campañas de sensibilización y cultura de seguridad digital.

El cumplimiento y seguimiento de estas acciones asegura la vigencia, eficacia y mejora progresiva del sistema, garantizando que la seguridad y privacidad de la información se mantengan alineadas con los objetivos institucionales, las normas nacionales y las políticas de Gobierno Digital.

7. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS			
ACTIVIDADES QUE SUFRIERON CAMBIOS	**CAMBIOS EFECTUADOS**	**FECHA DE CAMBIO**	**VERSIÓN**
Creación del documento	Creación del Documento	12/12/2024	001
Actualización del documento	Se actualizaron las siguientes secciones: • Introducción • Objetivo • Alcance • Definiciones • Metodología Se incluyeron nuevas secciones: • Objetivos específicos • Marco legal • Etapa 4: Mejora continua • Control de cambios	10/11/2025	002