PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Centro Nacional de Memoria Histórica

2026-2027

	NOMBRE	CARGO	FECHA
ELABORÓ	Angelica María Angel Jair Adel Caicedo	Contratistas Gestión 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

Centro Nacional de Memoria Histórica

Tabla de Contenido

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. INTRODUCCION

El Centro Nacional de Memoria Histórica (CNMH) reconoce la importancia de la información como activo estratégico para el cumplimiento de su misión. La protección de los activos de información, en cualquiera de sus estados, es fundamental para garantizar la confidencialidad, integridad y disponibilidad de los datos institucionales. Este Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026–2027 establece las acciones necesarias para reducir la probabilidad de materialización de amenazas, mitigar vulnerabilidades y asegurar el cumplimiento de los lineamientos definidos en el Modelo de Seguridad y Privacidad de la Información (MSPI), la norma ISO/IEC 27001:2022 y la Política de Gobierno Digital.

2. OBJETIVO GENERAL

Establecer las medidas necesarias para tratar los riesgos de seguridad y privacidad de la información, garantizando la protección de los activos y el cumplimiento normativo.

2.1 OBJETIVOS ESPECIFICOS

- Gestionar los riesgos de seguridad y privacidad de la información de acuerdo con la metodología definida por el DAFP alineado con la norma ISO/IEC 27001:2022.
- Fortalecer la cultura organizacional frente a la gestión de riesgos de seguridad y privacidad.
- Implementar los controles de seguridad de la información.
- Cumplir con los requisitos del MSPI y con la normativa nacional en materia de seguridad digital.

3. 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 tales como: la información, el software, elementos físicos, los servicios, las personas e intangibles.

Activo de información: Todo elemento que contiene o soporta información que tiene valor para la entidad y que debe ser protegido para garantizar su confidencialidad, integridad y disponibilidad. [Fuente: MSPI 2025]

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

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

Control: Medida que modifica un riesgo. [Fuente: ISO 27000]

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

Impacto: Consecuencia o efecto que la materialización de un riesgo puede tener sobre los objetivos de la organización, incluyendo la afectación a la confidencialidad, integridad y disponibilidad de la información. [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.

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]

Probabilidad: Grado de posibilidad de que un incidente o amenaza explote una vulnerabilidad y cause un impacto sobre los activos de información. [Fuente: ISO 27000]

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]

Riesgos de seguridad de la información: Riesgo derivado de la pérdida de confidencialidad, integridad o disponibilidad de la información, asociado a la materialización de una amenaza sobre un activo o grupo de activos. [Fuente: ISO 27000]

Riesgo Inherente: Es el nivel de riesgo al que se expone un proceso, actividad o activo antes de aplicar cualquier medida de control o mitigación. Representa la vulnerabilidad natural de la entidad frente a amenazas o factores de riesgo, y constituye la base para determinar el riesgo residual. [Fuente: GUIA GESTION DEL RIESGO V7 DAFP]

Riesgo Residual: Es el nivel de riesgo que permanece después de aplicar los controles establecidos. Refleja la eficacia de las medidas implementadas y la exposición aceptada por la entidad dentro de su apetito de riesgo. [Fuente: GUIA GESTION DEL RIESGO V7 DAFP]

Seguridad de la información: Conjunto de acciones, controles y buenas prácticas destinadas a proteger los activos de información frente a riesgos que puedan afectar la confidencialidad, integridad o disponibilidad de los datos institucionales y su adecuada gestión. [Fuente: GUIA GESTION DEL RIESGO V7 DAFP]

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

4. MARCO NORMATIVO

Constitución Política de Colombia – Artículo 15: *Por el cual se reconoce* el derecho fundamental a la intimidad personal y familiar, así como a la protección de los datos personales, estableciendo la obligación del Estado de garantizar su respeto, tratamiento legítimo y protección frente a usos indebidos.
Ley 1581 de 2012 – Régimen General de Protección de Datos

Personales: *Por la cual se dictan disposiciones generales para la protección de datos personales*, regulando los principios, derechos y procedimientos que rigen el tratamiento de la información personal y la obligación de las entidades públicas y privadas de garantizar su seguridad y confidencialidad.

Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional: *Por medio de la cual se crea* la Ley de Transparencia y del Derecho de Acceso a la Información Pública, garantizando la publicidad de la información pública, la protección de datos personales y el equilibrio entre transparencia y reserva legal.

Decreto 1083 de 2015 – Decreto Único Reglamentario del Sector de la Función Pública;: Por el cual se expiden las normas relacionadas con la gestión y el desempeño institucional, incorporando políticas de Gobierno Digital y Seguridad Digital como pilares del fortalecimiento de la administración pública y de la gestión de información en el Estado.

Decreto 1008 de 2018 – Política de Gobierno Digital: Por el cual se establecen los lineamientos de la Política de Gobierno Digital, promoviendo la transformación digital de las entidades públicas mediante la gestión eficiente de la información, la seguridad digital, la interoperabilidad y el fortalecimiento de los servicios ciudadanos digitales.

Resolución 500 de 2021 – Estrategia de Seguridad Digital y Modelo de Seguridad y Privacidad de la Información (MSPI): Por la cual se adoptan los estándares, lineamientos y componentes del Modelo de Seguridad y Privacidad de la Información, como habilitador de la Política de Gobierno Digital, orientado al fortalecimiento de la confianza y la protección de los activos de información del Estado.

Documento CONPES 3995 de 2020 – Política Nacional de Confianza y Seguridad Digital: Por el cual se define la política pública orientada a promover la protección de los datos, la infraestructura crítica cibernética y la gestión de riesgos digitales, fortaleciendo la cooperación interinstitucional y las capacidades nacionales en materia de seguridad digital.

Decreto 338 de 2022 – Modelo de Gobernanza de Seguridad Digital: Por el cual se establecen los lineamientos del modelo de gobernanza de seguridad digital, los roles y responsabilidades de las entidades públicas, y los principios que guían la gestión coordinada de la seguridad y la privacidad de la información en el Estado colombiano.

Resolución 746 de 2022 – Modelo de Seguridad y Privacidad de la Información (MSPI): Por la cual se adopta el modelo que define los lineamientos, roles, controles y procedimientos mínimos para la protección de los activos de información, en cumplimiento de los principios de confidencialidad, integridad y disponibilidad.

Decreto 767 de 2022 – Política de Gobierno Digital: Por el cual se actualizan los lineamientos generales de la Política de Gobierno Digital, fortaleciendo la gestión de la seguridad digital, la protección de datos, la interoperabilidad, la participación ciudadana y la innovación tecnológica en las entidades del Estado.

Ley 2294 de 2023 – Plan Nacional de Desarrollo 2022–2026 Colombia Potencia Mundial de la Vida: Por la cual se adopta el Plan Nacional de Desarrollo, que incluye la seguridad digital y la gestión de la información como elementos estratégicos para la transformación del Estado, la protección de los derechos digitales y la modernización tecnológica del sector público.
Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (DAFP, 2025): Por la cual se actualizan los lineamientos para la identificación, análisis, valoración, tratamiento y monitoreo de riesgos en las entidades públicas, integrando la gestión del riesgo digital, la seguridad de la información y la articulación con los estándares internacionales ISO 31000 e ISO/IEC 27005.
ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información (SGSI): Por la cual se establecen los requisitos internacionales para implementar, mantener y mejorar un sistema de gestión de seguridad de la información, garantizando la protección de los activos, la gestión de riesgos y la mejora continua del desempeño en seguridad.
ISO/IEC 27005:2022 – Gestión de Riesgos de Seguridad de la Información: Por la cual se proporcionan las directrices para el análisis y tratamiento de riesgos de seguridad de la información, articuladas con los principios de la gestión integral del riesgo definidos en la ISO 31000.

5. ALCANCE

El presente plan aplica a todos los procesos misionales, estratégicos, de apoyo y de evaluación del CNMH, así como a funcionarios, contratistas, proveedores y terceros que administren o traten activos de información institucionales, físicos o digitales, dentro o fuera de la infraestructura tecnológica de la Entidad.

6. PLAN DE TRATAMIENTO

Plan de Tratamiento de Riesgos de Seguridad de la Información						
Activo	**Opción de Tratamiento del Riesgo**	**Descripción tratamiento**	**Soporte**	**Fecha Inicio**	**Fecha Fin**	**Responsable**
Servidores y almacenamientos Centro de Datos (Dirección administrativa y Financiera - Gestión de TIC Transversal a todos los procesos del CNMH)	Evitar	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 de los sistemas de información e infraestructura crítica, así como la configuración de sistemas de monitoreo y correlación de alertas tempranas que permitan detectar fallas en la infraestructura tecnológica. Adicionalmente, se fortalecerán los controles de acceso físico al cuarto de servidores.	* Contrato con proveedor. * Plan de mantenimientos preventivo/correctivo. * Escenarios de redundancia (sistemas de información e infraestructura crítica) * Monitoreo y correlación de alertas tempranas. * Fortalecimiento de los controles de acceso físico al cuarto de servidores.	oct-25	dic-27	Gestión de TIC

Plan de Tratamiento de Riesgos de Seguridad de la Información						
Activo	**Opción de Tratamiento del Riesgo**	**Descripción tratamiento**	**Soporte**	**Fecha Inicio**	**Fecha Fin**	**Responsable**
Servidores y almacenamientos Centro de Datos (Dirección administrativa y Financiera - Gestión de TIC Transversal a todos los procesos del CNMH)	Evitar	Se llevará a cabo un plan de tratamiento orientado a fortalecer la disponibilidad de la información y los servicios tecnológicos ante fenómenos climáticos mediante el robustecimiento de los controles ambientales y la protección eléctrica de la infraestructura. Se debe realizar la instalación y calibración de sensores de temperatura, humedad e inundación en el Centro de Datos y áreas críticas, complementado con alarmas de alerta temprana integradas a un sistema de monitoreo para la detección oportuna de variaciones ambientales que integre registros de monitoreo continuo.	* Contrato con proveedor. * Instalación de sensores ambientales. * Calibración y pruebas de funcionamiento de los sensores. * Configuración de alertas tempranas. * Registro de monitoreo ambiental.	oct-25	dic-27	Gestión de TIC
Infraestructura de servidores y almacenamiento contratada en nube pública	Evitar	Para mitigar el riesgo asociado a la infraestructura de servidores y almacenamiento contratada en nube pública, se realizará una revisión de los contratos y acuerdos de nivel de servicio (SLA) para asegurar que contemplen disponibilidad mínima garantizada, tiempos de respuesta ante incidentes, mecanismos de soporte, replicación geográfica y responsabilidades compartidas de seguridad. De manera complementaria, se configurarán y validará los servicios de nube bajo lineamientos técnicos de buenas prácticas (ISO 27017), asegurando la implementación de alta disponibilidad, balanceo	* Contrato con proveedor. * Informe de revisión contractual y de SLA. * Matriz de responsabilidades compartidas. * Documento técnico de arquitectura y configuración cloud. * Registro de implementación o ajuste de configuraciones de seguridad. * habilitación de redundancia y balanceo de carga. * Pruebas de seguridad y validación de controles. * Registro de monitoreo y alertas.	oct-25	dic-27	Gestión de TIC

Plan de Tratamiento de Riesgos de Seguridad de la Información						
Activo	**Opción de Tratamiento del Riesgo**	**Descripción tratamiento**	**Soporte**	**Fecha Inicio**	**Fecha Fin**	**Responsable**
		de carga, redundancia de almacenamiento y replicación entre zonas, reduciendo así los puntos únicos de falla. Asimismo, se corregirán configuraciones inseguras mediante controles de acceso adecuados y revisión de permisos.				
Información Clasificada y Reservada.	Mitigar	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.	* Revisión y actualización de controles de acceso a sistemas y repositorios que contengan información pública, clasificada y reservada. * Procedimiento de autenticación Multifactor (MFA). * Fortalecer la implementación del MFA. * Indicadores de implementación y puesta en marcha del MFA (porcentaje de usuarios con MFA activo). * Inventario y clasificación de los repositorios que contienen información reservada y clasificada. * Capacitación a los usuarios sobre el uso del MFA.	oct-25	dic-27	Gestión de TIC
Información Clasificada y Reservada.	Mitigar	El CNMH implementará un proceso de copias de seguridad totalmente automatizado con el fin de mitigar el riesgo asociado a la realización manual de respaldos, fortaleciendo la disponibilidad e integridad de la información institucional. Para ello, se adoptará una herramienta	* Contrato con proveedor. * diseño del nuevo esquema de copias de seguridad. * Acta de instalación y configuración inicial de la herramienta de Backup. * Definición formal de políticas de Backup. * Programación	oct-25	dic-27	Gestión de TIC

Plan de Tratamiento de Riesgos de Seguridad de la Información						
Activo	**Opción de Tratamiento del Riesgo**	**Descripción tratamiento**	**Soporte**	**Fecha Inicio**	**Fecha Fin**	**Responsable**
		centralizada de Backup que permita programar respaldos periódicos, verificación automática de integridad, cifrado de los datos y generación de alertas ante fallos en la ejecución. Asimismo, se documentará un procedimiento técnico que defina la frecuencia, los tipos de respaldo, los responsables operativos y los mecanismos de restauración, acompañado de pruebas periódicas de recuperación para garantizar la continuidad operativa ante incidentes. Este plan permitirá reducir errores humanos, asegurar trazabilidad y mejorar la eficiencia en la gestión de copias de seguridad del CNMH.	automatizada de copias de seguridad. * Registro de logs y reportes de ejecución. * Procedimiento técnico documentado de copias de seguridad y restauración. * Pruebas de restauración y recuperación de datos. * Capacitación al personal responsable			
* Servidor MySQL base de datos SAIA. * Servidor Aplicación SAIA 8. * SAIA Producción. * Oracle Base Datos SAIA.	Mitigar	Este plan incluye la documentación y estandarización de los procedimientos críticos de uso, la implementación de controles de validación y doble verificación en actividades sensibles, la creación de ambientes de prueba para validar configuraciones antes de pasarlas a producción y la capacitación continua de los usuarios responsables de la operación del sistema.	* Contrato con proveedor. * Inventario de procedimientos críticos. * Estandarización de actividades sensibles. * Implementación de ambientes de prueba. * Procedimiento de gestión de cambios.	oct-25	dic-27	Gestión de TIC

7. ARTICULACION CON OTROS INSTRUMENTOS

El presente plan se articula con los siguientes instrumentos institucionales:

- Plan de Seguridad y Privacidad de la Información (PSPI).
- Matriz de Riesgos de Seguridad y Privacidad de la Información.
- Plan Estratégico de Seguridad y Privacidad de la Información (PESI).
- Matriz de Activos de Información.

8. 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 general • Se incluyeron definiciones • Alcance Se incluyeron nuevas secciones: • Objetivos específicos • Marco legal • Planificación de actividades • Articulación con otros instrumentos • Control de cambios	02/12/2025	002