Centro Nacional de Memoria Histórica

# Plan de Mantenimiento Tecnológico 2021

## Centro Nacional de Memoria Histórica

# Plan de Mantenimiento Tecnológico

# Centro Nacional de Memoria Histórica

## Contenido

## 1. Contexto de la entidad

El Centro Nacional de Memoria Histórica (CNMH) fue creado por la Ley 1448 de 2011 *"Por la cual se dictan medidas de atención, asistencia y reparación integral a las víctimas del conflicto armado interno y se dictan otras disposiciones."*; es un establecimiento público del orden nacional, adscrito al Departamento Administrativo para la Prosperidad Social (DPS) mediante el Decreto 4158 de 2011 y con el Decreto 4803 de 2011 se estableció su estructura.

El CNMH tiene por objeto la recepción, recuperación, conservación, compilación y análisis de todo el material documental, testimonios orales y por cualquier otro medio, relativo a las violaciones ocurridas con ocasión del conflicto armado interno colombiano, a través de la realización de investigaciones, actividades museísticas, pedagógicas y otras relacionadas, que contribuyan a establecer y esclarecer las causas de tales fenómenos, conocer la verdad y contribuir a evitar en el futuro la repetición de los hechos. La información que acopia el CNMH debe ponerse a disposición de las víctimas, investigadores y de los ciudadanos en general, para enriquecer el conocimiento de la historia política y social de Colombia.

Por último, es importante precisar que la Ley 1448 tiene una vigencia de 10 años, y que el CNMH se creó en el marco de esta Ley, en consecuencia, el PETI, cuya vigencia inicial abarcó las vigencias 2017 a 2020, se extiende para abarcar la vigencia 2021**.**

## 2. Objetivo:

- Mantener la plataforma tecnológica, (Hardware y software tanto local como en nube) en condiciones óptimas para su utilización y aprovechamiento por parte de los usuarios (Funcionarios y contratistas) en la ejecucion de sus labores misionales como de apoyo.
- Mantener control de usuarios, accesos, bases de datos, conexiones remotas, carpetas compartidas en red y estado de contratos de soporte, que permitan prevenir, mitigar y corregir fallas o daños, relacionados con la plataforma tecnológica del CNMH.

## 3. Objetivos Específicos:

- Definir las fechas para la realización de los mantenimientos preventivos a los servicios tecnológicos del CNMH.
- Identificar los responsables de cada actividad a realizar
- Medir los niveles de desempeño de los servicios tecnológicos, garantizando un óptimo funcionamiento en todas las áreas del CNMH.

## 4. Definiciones

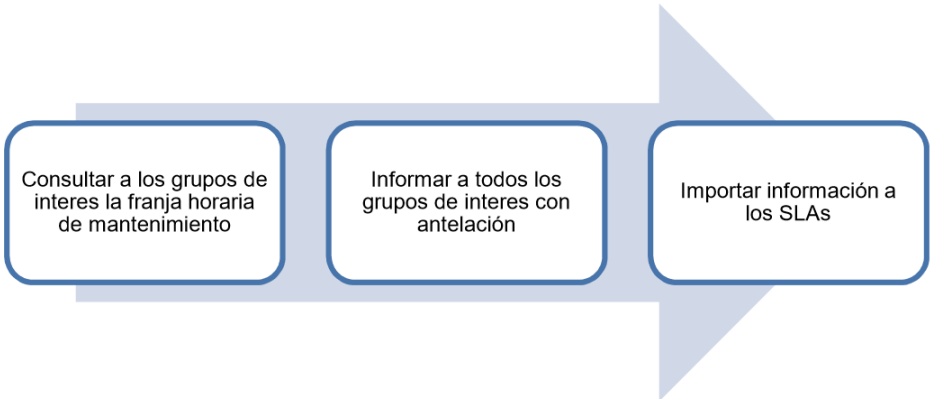
- **Disponibilidad**: Acceso y uso de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Confidencialidad**: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados
- **Información**: Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje
- **Dato**: Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Copias de respaldo**: Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
- **Carpetas Compartidas**: es básicamente igual que una carpeta normal salvo que su contenido será accesible para todos los usuarios que pertenezcan a un mismo grupo de trabajo.
- **Acuerdo de Nivel de Servicio (ANS**): Es un convenio entre un proveedor de servicios de TI y un cliente. describe las características del servicio de TI, los niveles de cumplimiento y las penalizaciones, y especifica las responsabilidades del proveedor y del cliente. Un ANS puede cubrir múltiples servicios de TI o múltiples clientes.
- **Data Center**: Es un “centro de datos” o “Centro de Proceso de Datos”, Los datos son almacenados, tratados y distribuidos al personal o procesos autorizados para consultarlos y/o modificarlo

- **Mantenimiento**: Es un proceso mediante el cual se asegura que un activo (equipo) continúe desempeñando las funciones deseadas.
- **Grupo de Sdoporte**: Es un equipo de profesionales dedicados a gestionar una variedad de eventos sobre el servicio. La mesa puede ser un punto único de contacto para los usuarios de TI. Maneja los incidentes y solicitudes de servicio a través del uso de herramientas especializadas para dejar registro y administrar los eventos.
- **Servidor Virtual**: Una partición dentro de un servidor que habilita varias máquinas virtuales dentro de dicha máquina por medio de varias tecnologías. Si necesita alojar múltiples sitios web, un Servidor Virtual Privado (VPS) es la opción más económica.
- **Storage (almacén)**: Bocablo en idioma Inglés comunmente utilizado para dar nombre a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador (servidor) con computadoras personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un sistema operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

## 5. Condiciones Generales

Para la realización del plan de mantenimiento del CNMH, se tuvo en cuenta la guía de servicios tecnológicos del Marco de Referencia de Arquitectura Empresarial de MinTIC para los siguientes pasos:

Gráfica 1. Procesos de planeación de mantenimiento.




Fuente: MinTIC, Guía de servicios tecnológicos, G.ST.01

Los tipos de mantenimiento que brinda La Dirección Administrativa y Financiera en su función de Gestión de TIC del CNMH son:

- **Correctivo.**

El mantenimiento correctivo se realiza de manera forzosa e inesperada, cuando ocurre un fallo y que impone la necesidad de reparar el equipo antes de continuar haciendo uso del mismo. En este sentido, el mantenimiento correctivo contingente implica que la reparación se lleve a cabo con la mayor rapidez para evitar daños materiales y humanos, así como pérdidas económicas.

- **Preventivo.**

El mantenimiento preventivo se hace con anticipación y de manera programada con el fin mitigar incidentes que puedan generar riesgos para la operación de la entidad, el mantenimiento preventivo consiste en dar limpieza general al equipo de cómputo y confirmar su correcto funcionamiento, en el caso de los computadores, el mantenimiento puede dividir en dos, el que se le da al equipo (físico) hardware y el que se les da a los programas instalados (lógicos) software.

## 5.1. Responsabilidad.

**CNMH:**
El profesional especializado de la Dirección Administrativa y Financiera - Gestión de TIC, será el responsable de asegurar que el personal que realice las labore de mantenimiento cuente con los conocimientos y habilidades necesarios para desempeñar la labor adecuadamente y realizar el seguimiento estratégico de la implementación del plan de mantenimientos.

**Equipo de trabajo de Gestión de TIC**:
Implementar los mantenimientos preventivos y correctivos a los servicios tecnológicos de la entidad de acuerdo con las fechas estipuladas.
Responder a las solicitudes de ocurrencia de eventos, para mitigar los riesgos.
Informar del correcto uso a los diferentes usuarios de los servicios tecnológicos.
Identificar las actividades de soporte que presta el personal del CNMH de acuerdo con los acuerdos de nivel de servicio (ANS) establecidos.

**Usuarios**:
Es responsabilidad de cada usuario el buen uso y manejo que se le dé a los servicios tecnológicos (hardware y software).
Mantener la confidencialidad de los respectivos usuarios y contraseñas de acceso y los privilegios, otorgados por Gestión de TIC, sobre las diferentes plataformas, sistemas y aplicaciones.

## 5.2. Control de Usuarios y Acceso a los SI y aplicaciones software:

El mantenimiento de la plataforma tecnológica del CNMH permitirá identificar los usuarios activos, el rol y privilegios de acceso de cada uno.
El control del acceso involucra a los usuarios de los sistemas informáticos específicos de la entidad.

Con el control de Acceso posibilita:

- Impedir el acceso no autorizado a los sistemas de información, base de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Registrar y revisar eventos y actividades criticas llevadas por los usuarios de los sistemas.
- Tener una concientización por parte de los usuarios sobre la responsabilidad respecto a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utiliza equipos móviles y equipos de trabajo remoto.

### 5.3. Lineamientos para el control de acceso a plataforma tecnológica

- **Creación de cuenta de usuario**: La generación de cuenta de usuario se realizará posterior a la solicitud realizada por la dependencia encargada, estas cuentas son personales e intransferibles y el usuario es el responsable del uso de la cuenta, así como también la seguridad de la contraseña, se autoriza el acceso físico y acceso a servicios de tecnologías de información.
- **Perfiles de Navegación de Internet**: Usuarios autorizados para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos de la Entidad o que afecten la seguridad de la información de la Entidad.
- **Acceso a Sistemas, aplicaciones y servicios web**: Se tendrán en cuenta los perfiles y roles según las necesidades de cada dirección misional y de apoyo para el acceso a la plataforma tecnológica y sistemas de información, con el fin de tener un control de solicitud, modificación, eliminación y/o inactivación de usuarios privilegiados o temporales.
- **Acceso Remoto**: La conexión remota a la red de área local de la Entidad debe ser establecida a través de una conexión VPN segura autorizada y configurada por personal de la Dirección Administrativa y Financiera – Gestión de TIC, que cuenta con el monitoreo y registro de las actividades necesarias, la autenticación de usuarios remotos deberá ser aprobada por el Jefe de dependencia o respectivo el Director, se efectúa el seguimiento a los accesos realizados por los usuarios, con el fin de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información.
- **Acceso a unidades de red o carpetas virtuales**: La Dirección Administrativa y Financiera – Gestión de TIC tiene implementado y configurado unidades de red o carpetas virtuales que permiten el almacenamiento de información digital para los usuarios de la entidad, así como las medidas de seguridad que permitan mantener la disponibilidad e integridad de la información allí almacenada. Los propietarios de los datos, son los responsables del contenido de los mismos y deben garantizar la disponibilidad, confidencialidad e integridad de la información que se encuentra almacenada en el servidor.
- **Acceso a servicios de la Entidad**:Todos los usuarios a quienes se les otorgue autorización de acceso a los servicios tecnológicos que presta la entidad son responsables del uso de estos servicios, así como de sus credenciales de acceso.
- **Depuración y Backup de la Información**: La Dirección Administrativa y Financiera – Gestión de TIC dispone y controla la ejecución de las copias de seguridad como medio de respaldo de la información de la Entidad, respaldo que garantizan la disponibilidad de toda la información y del software crítico. Se tiene definido un esquema de respaldo de la información. Se prueban los procedimientos de restauración, y así se asegura que son efectivos y que pueden ser ejecutados en los tiempos establecidos.
- **Actualización de S.O.:** Corregir o actualizar el software base de los servidores donde se alojan las aplicaciones misionales ubicadas en el Centro de Datos, a través de la instalación de parches con el fin de garantizar su operación. En los que aplique se deben tener en cuenta los conceptos técnicos del proveedor.
- **Contratos de Soporte de SI – Proveedores**: La Dirección Administrativa y Financiera – Gestión de TIC valida el estado de la contratación de las aplicaciones contratadas con terceros, la vigencia del soporte respectivo y se encarga de hacer seguimiento para garantizar el cumplimiento de las actividades contratadas.

## 6. Mantenimiento de la plataforma física.

Centro Nacional de Memoria Histórica

Teniendo en cuenta las necesidades de los servicios tecnológicos del CNMH, las siguientes corresponden a las actividades a ejecutar por parte del equipo de TI sobre la plataforma física:

- Verificar que todo software instalado en los equipos de propiedad del CNMH cuente con los respectivos soportes de licenciamiento y/o autorizaciones para su uso por parte del CNMH.
- Revisar el estado actual del equipo de cómputo, y en caso de ser necesario gestionar la garantía con el proveedor correspondiente.
- Iniciar el proceso de limpieza de cada uno de los equipos informáticos, e impresoras.
- Revisar el estado actual del antivirus, comprobar si esta con la respectiva licencia y firmas actualizadas.
- Desinstalar todo el software que no disponga de correspondiente licencia.
- Revisar demás equipos de cómputo, hardware y sus periféricos, y si hay que cambiar algo debe ser debidamente justificado, y reportado, para la sustitución o cambio de partes.
- Se debe reportar los mantenimientos en el aplicativo de Soporte correspondiente, por parte del técnico.

### 6.1. Actividades y fechas estimadas.

A continuación, se presenta el cronograma general de mantenimientos preventivos para los servicios tecnológicos del CNMH en la vigencia respectiva, de la misma manera se anexa el plan detallado de actividades de mantenimiento:

**Plan de mantenimiento de la plataforma física**

| Actividad de Mantenimiento | Periodicidad | Mes de ejecución |
|---|---|---|
| Mantenimiento preventivo y correctivo, equipos de cómputo. | Semestral | Junio 1 – Final primer mantenimiento del año.<br>Diciembre 1 – Final segundo mantenimiento del año. |
| Mantenimiento preventivo Datacenter, Servidores, Storage, Networking. | Semestral | Marzo 1 – Final primer mantenimiento del año.<br>Octubre 1 – Final segundo mantenimiento del año. |
| Mantenimiento preventivo/correctivo servidores virtuales | Semestral | Abril 1 – Final primer mantenimiento del año.<br>Octubre 1 – Final segundo mantenimiento del año. |

### 6.2. Seguimiento y Monitoreo:

El cronograma de mantenimientos se ejecutará en el lugar de trabajo y se acordará con el usuario la realización del mismo para no afectar las actividades diarias de los usuarios.

El técnico reportará al coordinador de soporte el respectivo informe correspondiente al mantenimiento, para después realizar acciones que permitan mejorar y el plan de acción correspondiente.

### 6.3. Riesgos:

Algunos de los riesgos que se pueden presentar en la ejecución del plan de mantenimientos son:

- Falta de herramientas como repuestos para cambio durante el mantenimiento.
- Disponibilidad de recursos humanos para la realización del mantenimiento.
- Incumplimiento en los tiempos de respuesta.
- Sucesos imprevistos ajenos a la Entidad (Por ejemplo: problemas del servicio de energía).
- Reporte a destiempo de las fallas por parte de los usuarios.

## 7. Mantenimiento de la plataforma virtual.

A continuación, se presenta el cronograma general de mantenimientos preventivos para los servicios tecnológicos del CNMH anualmente, de la misma manera se anexa el plan detallado da actividades de mantenimiento:

| Actividad de Mantenimiento | Periodicidad | Mes de ejecución |
|---|---|---|
| **Usuarios de Dominio** | Semestral | Marzo – Primer semestre<br>Septiembre- Segundo semestre |
| **Perfiles de Navegación Internet** | Semestral | Marzo – Primer semestre<br>Septiembre- Segundo semestre |
| **Acceso a Sistemas, aplicaciones y servicios web** | Semestral | Marzo – Primer semestre<br>Septiembre- Segundo semestre |
| **Acceso Remoto** | Semestral | Marzo – Primer semestre<br>Septiembre- Segundo semestre |
| **Acceso a Unidades de Red** | Semestral | Marzo – Primer semestre<br>Septiembre- Segundo semestre |
| **Depuración BD y Backup de la Información** | Semestral | Marzo – Primer semestre<br>Septiembre- Segundo semestre |
| **Actualización de S.O.** | Cuando sea requerido por la máquina y/o Proveedor | Por demanda. |
| **Catálogo de S.I** | Anual | 15 de noviembre |
| **Contratos de Soporte SI** | Seguimientos según las obligaciones contractuales. | Por demanda. |

### 7.1. Seguimiento y Monitoreo:

El cronograma de mantenimientos preventivos de los Sistemas de Información, se ejecutará en el lugar de trabajo y se acordará con los involucrados la realización del mismo para no afectar las actividades diarias de los usuarios.