



**SUBDIRECCIÓN ADMINISTRATIVA
UNIDAD DE INFORMÁTICA
GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
HOSPITAL MILITAR CENTRAL - HOMIL
CÓDIGO: GT-UNIN-PO-02
VERSIÓN: 01
FECHA DE EMISIÓN: 07-10-2025**

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES



POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Coronel Fernando Antonio Diaz Muñetón

Subdirector Administrativo
Subdirección Administrativa
Hospital Militar Central

TC Eduardo Enrique Mendoza Palacio

Jefe Unidad de Seguridad y defensa
Unidad de Informática
Hospital Militar Central

Ingeniero Jorge Manuel Puerto Gualteros

Ingeniero Especialista Seguridad
Unidad de Informática
Hospital Militar Central



TABLA DE CONTENIDO

1. INTRODUCCIÓN	4
2. OBJETIVO	4
2.1 OBJETIVO GENERAL	5
2.2 OBJETIVO ESPECÍFICO	5
3. ALCANCE	5
4. DECLARACIÓN DE POLÍTICA	6
5. MARCO LEGAL	6
6. JUSTIFICACIÓN	7
6.1 METODOLOGÍA	8
6.2. EJES ESTRATÉGICOS	10
7. GENERALIDADES	13
7.1. DEFINICIONES	13
7.2. ASPECTOS GENERALES INSTITUCIONALES	15
7.3. OTROS ASPECTOS	19
8. ROLES Y RESPONSABILIDADES	20
9. IMPLEMENTACIÓN	22
10. SEGUIMIENTO	23
12. COMUNICACIÓN Y CONSULTA	28
13. BIBLIOGRAFÍA	28
14. ANEXOS	29
15. CONTROL DE CAMBIOS	30



1. INTRODUCCIÓN

La presente Política de Protección de Datos Personales del Hospital Militar Central aborda un tema de vital importancia en la era digital actual. En un entorno donde los datos son un activo valioso y sensible, especialmente en el ámbito de la salud, comprender y aplicar esta política es fundamental para garantizar la privacidad y la confianza de todos los individuos que interactúan con nuestra institución. Invitamos a la lectura de este documento para conocer los pilares que rigen nuestra gestión de la información personal.

El interés primordial para la creación e implementación de esta política surge de la imperativa necesidad de cumplir con el marco legal colombiano vigente en materia de protección de datos personales, así como de adoptar las mejores prácticas en seguridad de la información. Su relevancia se magnifica en el contexto hospitalario, donde se manejan datos sensibles relacionados con la salud de pacientes, lo que exige un rigor ético y técnico excepcional. Esta política busca asegurar la confidencialidad, integridad y disponibilidad de la información, impactando directamente en la calidad del servicio, la seguridad de los pacientes y la reputación del Hospital Militar Central.

Para la elaboración de este documento, se empleó una metodología sistemática y estructurada. Se realizó una evaluación diagnóstica exhaustiva del estado actual de la gestión de datos en el Hospital Militar Central, analizando la normativa aplicable, las prácticas preexistentes y los riesgos inherentes al sector de la salud. La estrategia se centró en la identificación del marco normativo, la definición de principios rectores, la asignación de responsabilidades claras y el establecimiento de controles de seguridad técnicos, humanos y administrativos. Este enfoque busca no solo el cumplimiento normativo, sino también la construcción de una cultura organizacional basada en el respeto por la privacidad.

2. OBJETIVO

Para materializar esta política, el Hospital Militar Central, fija los siguientes objetivos:

○ 2.1 OBJETIVO GENERAL

El objetivo de la presente política es establecer los lineamientos, principios, responsabilidades y procedimientos transversales para asegurar la adecuada protección de los datos personales que recolecta, usa, almacena y circula en el Hospital Militar Central, mediante la implementación de controles técnicos,



administrativos y humanos que garanticen el cumplimiento del marco normativo colombiano vigente y el ejercicio efectivo del derecho fundamental al Habeas Data por parte de los titulares.

○ **2.2 OBJETIVO ESPECÍFICO**

- Definir e implementar procedimientos y controles esenciales para la recolección, almacenamiento, uso, circulación y supresión de datos personales. Esto asegurará la licitud, lealtad y transparencia en el tratamiento de la información, garantizando el consentimiento informado de los titulares y la estricta confidencialidad de los datos, especialmente los sensibles.
- Capacitar y sensibilizar a todo el personal del Hospital Militar Central sobre la importancia de la protección de datos personales y las responsabilidades que les incumben, con el fin de fomentar una cultura organizacional de respeto a la privacidad, a través de programas de formación continuos y materiales educativos accesibles.
- Garantizar el ejercicio efectivo de los derechos de los titulares de datos personales (acceso, rectificación, supresión, actualización y revocación del consentimiento), para fortalecer la confianza en la gestión de la información, implementando canales de atención claros y eficientes para consultas y reclamos.
- Minimizar los riesgos asociados al tratamiento de datos personales sensibles, como los de salud y biométricos, proporcionando un marco de seguridad robusto que prevenga accesos no autorizados, fugas o usos indebidos, mediante la aplicación de medidas de seguridad técnicas, humanas y administrativas alineadas con las mejores prácticas y la normativa vigente.

3. ALCANCE

La presente Política de Protección de Datos Personales del Hospital Militar Central establece un marco de aplicación que abarca todas las bases de datos, sin importar su formato (físico o digital), en las que el Hospital Militar Central actúe como responsable del tratamiento de datos personales. Su cobertura se extiende a la totalidad del ciclo de vida del dato, desde el momento de su recolección inicial hasta su eventual supresión definitiva.



- En términos de alcance institucional, esta política es de obligatorio cumplimiento para todo el personal vinculado al Hospital Militar Central, incluyendo funcionarios públicos, militares en comisión, personal en modalidad de OPS, personal tercerizado y sus colaboradores que accedan a datos personales, así como el personal en formación, cualquier otra persona natural o jurídica autorizada que participe o apoye en el desarrollo de proyectos, actividades o procesos institucionales.
- Respecto a los titulares de los datos, esta política aplica al tratamiento de la información personal de pacientes, sus familias, acompañantes, empleados, exempleados, aspirantes a cargos, contratistas, proveedores, visitantes y cualquier otro titular cuyos datos sean gestionados por el Hospital Militar Central.
- Desde una perspectiva de procesos y objetivos estratégicos, la política se integra transversalmente en la operación del Hospital Militar Central, buscando fortalecer la gestión por procesos y la cultura de mejoramiento continuo. Se alinea con el Marco General del Modelo Integrado de Planeación y Gestión (MIPG) en lo relacionado con la política de seguridad digital y contribuye directamente al objetivo estratégico institucional de "Fortalecer la gestión por procesos y cultura de mejoramiento". Su alcance, por tanto, delimita la forma en que el Hospital Militar Central gestiona la privacidad y seguridad de la información personal en todas sus actividades, asegurando el cumplimiento normativo y la protección de los derechos fundamentales de los titulares.

4. DECLARACIÓN DE POLÍTICA

El Hospital Militar Central asume el firme compromiso de proteger los datos personales que recolecta, usa, almacena y circula, reconociendo su importancia fundamental para la garantía del derecho a la privacidad y el Habeas Data de todos los titulares. La implementación de esta Política Institucional es crucial para asegurar la confidencialidad, integridad y disponibilidad de la información, especialmente la sensible relacionada con la salud. Constituye un pilar estratégico en el mejoramiento continuo de nuestros procesos y en la prestación de servicios de salud de la más alta calidad, fortaleciendo la confianza de nuestros pacientes, usuarios y la comunidad en general.



5. MARCO LEGAL

Esta Política se fundamenta y se interpreta de acuerdo con las siguientes normas:

TIPO	No.	FECHA DE EXPEDICIÓN	ORIGEN	ORGANISMO EMISOR
Constitución		1991	Asamblea Nacional Constituyente	Artículo 15 (Derecho al Habeas Data) y Artículo 20 (Derecho a la Información)
Ley Est.	1581	17-oct-2012	Congreso de la República	Régimen General de Protección de Datos Personales en Colombia.
Ley Est.	1712	06-mar-2014	Congreso de la República	Ley de Transparencia y Acceso a Información Pública (Aplicable en lo pertinente).
Ley	1266	31-dic-2008	Congreso de la República	Regula Habeas Data para información financiera, crediticia, comercial (Aplicable en lo pertinente).
Decreto	1377	27-jun-2013	Presidencia de la República / MinCIT	Reglamenta parcialmente la Ley 1581 (Autorización, Políticas, Avisos, Transferencias).
Decreto	886	13-may-2014	Presidencia de la República / MinCIT	Reglamenta el Registro Nacional de Bases de Datos (RNBD). (Compilado en DUR 1074)
Decreto	1074 (DUR)	26-may-2015	Presidencia de la República / MinCIT)	Decreto Único Reglamentario Sector Comercio (Compila Decretos 1377 y 886 - Cap. 25 y 26).
Decreto	255	25-feb-2022	Presidencia de la República / MinCIT)	Modifica el DUR 1074/2015. Introduce Normas Corporativas Vinculantes (BCR) para transferencias internacionales.
Sentencia	c-748	06-oct-2011	Corte Constitucional	Revisión previa de constitucionalidad de la Ley Estatutaria de protección de datos.
Circular Única		2015 (compilada, actualizada hasta 2022)	Superintendencia de Industria y Comercio (SIC)	Instrucciones sobre protección de datos personales, Título V, Cap. Segundo.
Guía técnica		2021 (última actualización)	Superintendencia de Industria y Comercio (SIC)	Guía para la implementación del principio de Responsabilidad Demostrada (Accountability).

6. JUSTIFICACIÓN

La presente Política de Protección de Datos Personales del Hospital Militar Central se desarrolla y adopta en respuesta a las siguientes necesidades y obligaciones fundamentales:



- **Cumplimiento Normativo:** Dar estricto cumplimiento al marco legal colombiano vigente en materia de protección de datos personales, principalmente la Ley Estatutaria 1581 de 2012, sus decretos reglamentarios (como el 1377 de 2013), leyes modificatorias (Ley 2126 de 2021), circulares de la Superintendencia de Industria y Comercio (como la Circular Externa 002 de 2022) y demás normativa concordante, asegurando la protección del derecho fundamental al Habeas Data (Art. 15 de la Constitución Política).
- **Actualización y Unificación:** Actualizar, consolidar y unificar las directrices institucionales previamente existentes y versiones anteriores para reflejar la evolución normativa, las mejores prácticas y las necesidades operativas actuales del Hospital Militar Central.
- **Estandarización Institucional:** Alinear la gestión de la protección de datos personales con los lineamientos y estructuras documentales definidas por el Hospital Militar Central, adoptando el formato institucional para planes y políticas, garantizando coherencia y formalidad.
- **Gestión de Riesgos y Seguridad:** Establecer un marco claro y robusto para la gestión segura de la información personal, minimizando los riesgos asociados a su tratamiento (accesos no autorizados, fugas, pérdidas, usos indebidos), especialmente considerando la alta sensibilidad de los datos de salud manejados.
- **Garantía de Derechos:** Proveer un instrumento claro y accesible para que los titulares de los datos (pacientes, empleados, contratistas, etc.) conozcan sus derechos y los mecanismos para ejercerlos efectivamente ante el Hospital Militar Central.
- **Fomento de la Cultura de Protección de Datos:** Servir como herramienta fundamental para la capacitación, sensibilización y guía de todo el personal y terceros vinculados al Hospital Militar Central sobre sus responsabilidades en el correcto tratamiento de la información personal, promoviendo una cultura organizacional de respeto a la privacidad.

Este documento es esencial para garantizar que el Hospital Militar Central opere con los estándares de legalidad, seguridad, transparencia y respeto por los derechos fundamentales en todo lo concerniente a la Protección de datos personales.

○ **6.1 METODOLOGÍA**

La formulación de esta Política se llevó a cabo siguiendo una metodología sistemática y estructurada con el objetivo de perfeccionar la administración de la protección de datos en el Hospital Militar Central. El proceso inició con una



evaluación diagnóstica del estado actual, en la que se examinaron la normativa aplicable, las políticas y prácticas preexistentes, y los riesgos particulares inherentes al ámbito hospitalario. Se tomaron en cuenta tres dimensiones fundamentales: **Jurídica** (garantizar el acatamiento legal), **Operativa** (incorporar la protección en los procedimientos habituales) y **Cultural** (promover la sensibilización y la responsabilidad).

La estrategia global consistió en:

- **Identificación del Marco Normativo:** Recopilación y análisis detallado de leyes, decretos y circulares aplicables.
- **Definición de Principios y Lineamientos:** Establecimiento de los principios rectores (legalidad, finalidad, etc.) como base de toda actuación.
- **Determinación de Finalidades:** Identificación clara y legítima de los propósitos para los cuales el Hospital Militar Central trata datos personales.
- **Diseño de Procedimientos:** Creación de mecanismos claros para la obtención de autorización, atención de derechos de los titulares (consultas y reclamos), gestión de incidentes y transferencias/transmisiones.
- **Asignación de Responsabilidades:** Definición explícita de roles y deberes para las diferentes instancias y funcionarios del Hospital Militar Central.
- **Establecimiento de Controles:** Incorporación de medidas de seguridad técnicas, humanas y administrativas.
- **Alineación Institucional:** Adopción de la estructura y formato definidos por el Hospital Militar Central para sus políticas.

Esta metodología es flexible y adaptable, permitiendo revisiones periódicas para incorporar cambios normativos o mejoras identificadas. Integra el nivel **estratégico** (alineación con objetivos institucionales, cumplimiento legal), **táctico** (definición de procesos, asignación de roles) y **operativo** (ejecución diaria de procedimientos, aplicación de controles).

La presente Política se fundamenta y desarrolla a través de los siguientes componentes esenciales:

- **Principios Rectores:** Son la base ética y legal del tratamiento de datos (Legalidad, Finalidad, Libertad, Veracidad, Transparencia, Acceso y Circulación Restringida, Seguridad, Confidencialidad). Guían toda interpretación y aplicación de la Política.
- **Autorización y Consentimiento:** Mecanismos para obtener el consentimiento previo, expreso e informado del titular, especialmente crítico para datos sensibles.



- **Derechos de los Titulares:** Reconocimiento y facilitación de los derechos a conocer, actualizar, rectificar, suprimir datos, revocar autorización y acceder a la información.
- **Deberes del Responsable Hospital Militar Central:** Obligaciones que el Hospital Militar Central debe cumplir para garantizar la protección de datos.
- **Finalidades del Tratamiento:** Definición clara y específica de los usos permitidos para los datos recolectados.
- **Tratamiento de Datos Sensibles y de NNA (niños, niñas y adolescentes):** Reglas especiales y reforzadas para el manejo de información de salud, datos biométricos, y datos de menores de edad.
- **Procedimientos de Consultas y Reclamos:** Canales y plazos definidos para atender las solicitudes de los Titulares.
- **Medidas de Seguridad:** Controles técnicos, humanos y administrativos para proteger la información.
- **Gestión de Incidentes:** Protocolo para responder a posibles brechas de seguridad.
- **Transferencia y Transmisión:** Condiciones para compartir datos con terceros, dentro y fuera del país.
- **Registro Nacional de Bases de Datos (RNBD):** Cumplimiento de la obligación de registro ante la SIC.
- **Gobernanza de Datos:** Roles, responsabilidades y estructura para la supervisión y ejecución de la política.

○ 6.2. EJES ESTRATÉGICOS

6.2.1 POLÍTICAS, PLANES Y PROGRAMAS INTERNACIONALES, NACIONALES Y SECTORIALES

Lo contenido en la Política de Protección de Datos para el Hospital Militar Central está alineado con:

- Marco legal colombiano vigente en materia de protección de datos personales, principalmente la Ley Estatutaria 1581 de 2012, sus decretos reglamentarios (como el 1377 de 2013), leyes modificatorias (Ley 2126 de 2021).
- **Circular Única de la SIC** – Título V, Capítulo Segundo (instrucciones en protección de datos) y **Guía de Responsabilidad Demostrada (Accountability)** de la SIC (versión 2021).” Superintendencia de Industria y ComercioAlcaldía de Bogotá

6.2.3. MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN – MIPG

La Política de Protección de Datos para el Hospital Militar Central se encuentra alineada al Marco General del Modelo Integrado de Planeación y Gestión en lo relacionado con la política de gestión y desempeño institucional (Seguridad Digital).

6.2.4. PLAN ESTRATÉGICO INSTITUCIONAL



MISIÓN

Prestar servicios integrales especializados a los usuarios del Subsistema de Salud de las Fuerzas Militares centrados en el paciente y su familia y gestionar conocimiento a través de la academia y la investigación.



VISIÓN

El Hospital Militar Central continuará siendo la reserva estratégica de la nación en servicios integrales de salud y generación del conocimiento.

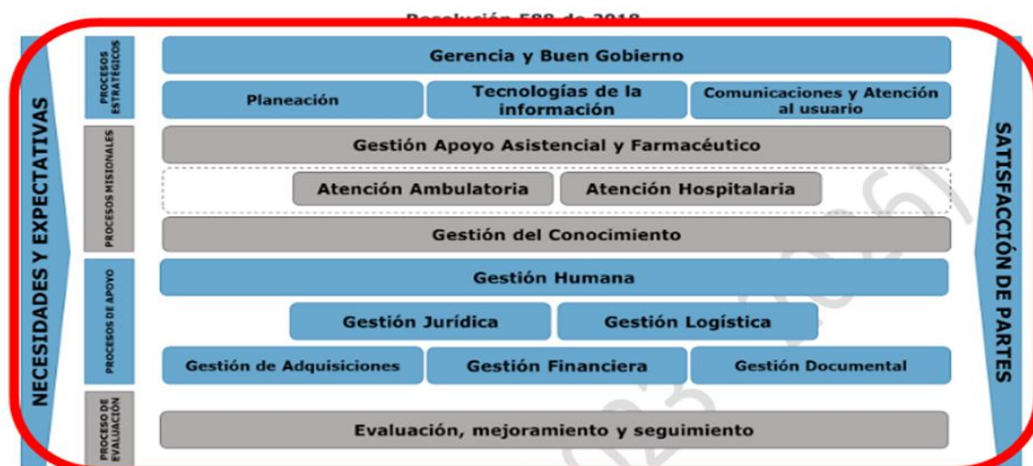
Con el objetivo de garantizar la protección de Datos Personales en el Hospital Militar Central, la Unidad de Informática - GSPI, en respaldo a los procesos institucionales, desarrolla la implementación de la Política de Tratamiento de Datos. Esto se realiza en cumplimiento de la exigencia del Gobierno Nacional respecto a la implementación de la política de Seguridad Digital, y con la intención de salvaguardar derechos fundamentales como el habeas data, la imagen, la intimidad, el buen nombre y la privacidad.

6.2.5. MAPA ESTRATÉGICO



La Política de Protección de Datos se enmarca a nivel de la entidad dentro del objetivo No 3 “Fortalecer la gestión por procesos y cultura de mejoramiento”, que busca que el Hospital Militar Central en concordancia con el proceso de fortalecimiento organizacional y el mejoramiento continuo de los procesos desarrolla acciones que facilitan el control y evaluación del cumplimiento a la normatividad, estándares de calidad en aras de asegurar y optimizar el tratamiento de datos personales de los pacientes, funcionarios, estudiantes, militares en comisión, contratista y cualquier colaborador del Hospital Militar Central.

6.2.6. MAPA DE PROCESOS





Hospital Militar Central fundamenta su funcionamiento en procesos organizacionales de carácter estratégico, misional, de apoyo y evaluación. Estos procesos se sustentan en la estandarización de procedimientos, guías y manuales, todos ellos enfocados en la prestación de servicios que se distinguen por su calidad, humanización y seguridad, dirigidos tanto a los usuarios como a la comunidad, y promovidos a través de una cultura de mejoramiento continuo. En consecuencia, la Política de Tratamiento de Datos se erige como un elemento transversal a la totalidad de los procesos llevados a cabo por la entidad.

6.2.7. ORGANIGRAMA



● 7. GENERALIDADES

○ 7.1. DEFINICIONES

Para los efectos de esta Política, se adoptan las siguientes definiciones, de conformidad con la Ley 1581 de 2012 y normas complementarias:

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de sus datos personales.
- **Aviso de Privacidad:** Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.



- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento (físico o digital).
- **Datos personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Dato Público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Dato Privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el Titular.
- **Dato Semiprivado:** Es aquel dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general. (Ej. Datos financieros).
- **Dato Sensible:** Aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación. Incluyen datos sobre origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos, organizaciones sociales, de derechos humanos, datos relativos a la salud, a la vida sexual y datos biométricos. El Hospital Militar Central, presta especial atención a esta categoría, dada su naturaleza hospitalaria.
- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.
- **PQRSDF:** Sistema que permite a los usuarios presentar Peticiones, Quejas, Reclamos, Sugerencias, Denuncias y Felicitaciones para expresar sus inquietudes o reconocer la calidad del servicio recibido.
- **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. Para efectos de esta política, el Hospital Militar Central es el Responsable.
- **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación, supresión, transferencia o transmisión.
- **Transferencia:** Envío de datos personales por parte del Responsable a un Receptor (que a su vez será Responsable), dentro o fuera del país.



- **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

○ **7.2. ASPECTOS GENERALES INSTITUCIONALES**

- **7.2.1. DESCRIPCIÓN DE LOS PROCESOS**
- **7.2.1.1. PROCESOS ESTRATÉGICOS**

ID	NOMBRE	OBJETIVO	RESPONSABLE
GB-DIGE-CP-01	Gerencia y Buen Gobierno	Definir los lineamientos generales, las políticas y la estructura de operación con el fin de garantizar el cumplimiento de la misión institucional.	Director General de Entidad Descentralizada Adscrita del Sector Defensa

Tabla 3. Gerencia y Buen Gobierno

ID	NOMBRE	OBJETIVO	RESPONSABLE
PL-DIGE-CP-05	Planeación	Definir las estrategias orientadas para el logro de la misión institucional, mediante la formulación de planes, programas y proyectos con el fin de garantizar la mejora continua en la prestación de los servicios.	Jefe de Oficina Asesora del Sector Defensa – Oficina Asesora de Planeación.

Tabla 4. Planeación

ID	NOMBRE	OBJETIVO	RESPONSABLE
GT-SUAD-CP-05	Tecnologías de la Información	Proyectar e implementar soluciones y servicios en tecnologías de información cumpliendo con los estándares normativos establecidos, que permitan el cumplimiento de los objetivos de la entidad de manera transparente y oportuna.	Jefe de Seguridad y Defensa - Unidad de Informática

Tabla 5. Tecnologías De La Información



ID	NOMBRE	OBJETIVO	RESPONSABLE
CA-DIGE-CP-03	Comunicaciones y Atención al usuario y relacionamiento ciudadano	Brindar atención y respuesta a las necesidades de las partes interesadas de acuerdo a la normatividad; propendiendo por el desarrollo de la gestión de las comunicaciones internas y externas, las cuales faciliten el cumplimiento de la misión institucional, la satisfacción de los usuarios y el posicionamiento de la entidad.	Director General de Entidad Descentralizada Adscrita del Sector Defensa

Tabla 6. Comunicaciones y Atención al usuario

■ 7.2.1.2. PROCESOS MISIONALES

ID	NOMBRE	OBJETIVO	RESPONSABLE
AA-SSAA-CP-02	Gestión Apoyo Asistencial y Farmacéutico	Contribuir a la atención médico asistencial a través de servicios de apoyo que permitan generar diagnósticos y tratamientos integrales	Subdirector del Sector Defensa – Subdirector de Servicios Ambulatorios y de Apoyo Diagnóstico

Tabla 7. Gestión Apoyo Asistencial y Farmacéutico

ID	NOMBRE	OBJETIVO	RESPONSABLE
AM-SSAA-CP-01	Atención Ambulatoria	Garantizar la atención integral (oportuna, segura y humanizada) en los servicios ambulatorios al paciente y su familia cumpliendo los estándares y contribuyendo al cumplimiento de la misión institucional	Subdirector del Sector Defensa – Subdirector de Servicios Ambulatorios y de Apoyo Diagnóstico

Tabla 8. Atención Ambulatoria



ID	NOMBRE	OBJETIVO	RESPONSABLE
AH-SUMD-CP-01	Atención Hospitalaria	Prestar la atención en los servicios de hospitalización de manera integral (segura, humanizada, oportuna y adecuada) cumpliendo con los requisitos previamente definidos de tal forma que contribuya a mejorar las condiciones de salud de los usuarios y apoyo al entorno familiar	Subdirector del Sector Defensa –Subdirección Médica

Tabla 9. Atención Hospitalaria

ID	NOMBRE	OBJETIVO	RESPONSABLE
GC-SDIC-CP-01	Gestión del Conocimiento	Identificar, producir y utilizar información interna para generar conocimiento que aporte al aprendizaje institucional, la mejora continua y al cumplimiento de la misión institucional	Subdirector Sector Defensa –Subdirección de Docencia e Investigación Científica

Tabla 10. Gestión del Conocimiento

■ 7.2.1.3. PROCESOS DE APOYO

ID	NOMBRE	OBJETIVO	RESPONSABLE
GH-SUAD-CP-03	Gestión Humana	Planear, ejecutar y controlar las acciones relacionadas con la administración y el desarrollo del Talento Humano gestionando las situaciones administrativas desde el ingreso, permanencia y retiro del personal para contribuir en el correcto funcionamiento de la entidad.	Jefe de Seguridad y Defensa - Unidad de Talento Humano

Tabla 11. Gestión Humana



ID	NOMBRE	OBJETIVO	RESPONSABLE
GJ-DIGE-CP-04	Gestión Jurídica	Asesorar y representar en asuntos jurídicos administrativos y judiciales internos y externos relacionados con las actividades desarrolladas en la Institución.	Jefe de Oficina Asesora del Sector Defensa – Oficina Asesora Jurídica

Tabla 12. Gestión Jurídica

ID	NOMBRE	OBJETIVO	RESPONSABLE
GL-SUAD-CP-04	Gestión Logística	Definir, coordinar y prestar los servicios de infraestructura, mantenimiento, hotelería (lavandería, aseo, alimentación) seguridad, transporte, y gestión ambiental requeridos por los clientes internos y externos	Jefe de Seguridad y Defensa - Unidad de Apoyo Logístico

Tabla 13. Gestión Logística

ID	NOMBRE	OBJETIVO	RESPONSABLE
GA-SUAD-CP-01	Gestión de Adquisiciones	Proveer bienes y servicios requeridos por el Hospital Militar Central contribuyendo así al cumplimiento de la misionalidad institucional de acuerdo con lo establecido por la ley.	Jefe de Seguridad y Defensa - Unidad de Compras, Licitaciones y Bienes Activos

Tabla 14. Gestión de Adquisiciones

ID	NOMBRE	OBJETIVO	RESPONSABLE
GF-SUFI-CP-01	Gestión Financiera	Ejecutar y controlar los recursos financieros de la entidad para el cumplimiento de la misión institucional de acuerdo a la normatividad vigente.	Subdirector del Sector Defensa –Subdirección Financiera

Tabla 15. Gestión Financiera



ID	NOMBRE	OBJETIVO	RESPONSABLE
GD-SUAD-CP-02	Gestión Documental	Administrar y controlar los diferentes documentos recibidos y producidos por la entidad, con el fin de dar tratamiento, conservación y disposición final, preservando la memoria institucional conforme a las disposiciones legales vigentes.	Jefe de Seguridad y Defensa - Unidad de Apoyo Logístico

Tabla 16. Gestión Documental

■ 7.2.1.4. PROCESOS DE EVALUACIÓN Y CONTROL

ID	NOMBRE	OBJETIVO	RESPONSABLE
EM-DIGE-CP-02	Evaluación, mejoramiento y seguimiento	Evaluar en forma independiente el Sistema de Control Interno de acuerdo con las normas vigentes y asesorar en el mejoramiento continuo del sistema, fortaleciendo la cultura del control para que la administración en todos sus niveles tomen las decisiones en cumplimiento de la misión institucional	Jefe de Oficina Control Interno

Tabla 17. Evaluación, mejoramiento y seguimiento

○ 7.3. OTROS ASPECTOS

PRINCIPIOS DEL TRATAMIENTO DE DATOS

El Hospital Militar Central cumplirá con los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

ACEPTACIÓN DE POLÍTICAS POR PARTE DEL TITULAR

El Hospital Militar Central obtendrá el consentimiento previo, expreso e informado del titular para el tratamiento de sus datos personales, salvo en los casos expresamente previstos por la ley. Este consentimiento se obtendrá por escrito, de forma verbal o mediante conductas inequívocas del titular que permitan concluir de manera razonable que ha otorgado su consentimiento.



INFORMACIÓN AL TITULAR

Al momento de solicitar el consentimiento, el Hospital Militar Central informará al titular de manera clara y suficiente sobre:

- La finalidad del tratamiento.
- Los derechos que le asisten como Titular.
- La identificación, dirección física o electrónica y datos de contacto del Responsable del Tratamiento.
- El carácter facultativo de la respuesta a las preguntas sobre datos sensibles.

TRATAMIENTO DE DATOS SENSIBLES

El tratamiento de datos sensibles requerirá el consentimiento previo, expreso e informado del Titular y deberá cumplir con los siguientes requisitos especiales:

- Informar al Titular que no está obligado a autorizar el tratamiento de dichos datos.
- Informar de forma explícita y previa cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad del mismo.

• 8. ROLES Y RESPONSABILIDADES

La responsabilidad por el cumplimiento de esta Política recae en todos los niveles del Hospital Militar Central. A continuación, se describen los roles y responsabilidades principales:

RESPONSABLE	QUÉ HARÁ (ACTIVIDADES PRINCIPALES)	OBJETIVO	CUÁNDO
Dirección General	Aprobar la Política y sus actualizaciones. Proveer los recursos necesarios para su implementación. Promover una cultura de protección de datos desde el más alto nivel.	Mediante acto administrativo de aprobación. Asignación presupuestal. Comunicación estratégica.	Al emitir/actualizar política. Anual (Presupuesto) . Continuo.
Oficial de Seguridad / o quien haga sus veces	Liderar, supervisar y coordinar la implementación y cumplimiento de la Política. Servir de enlace con la SIC. Gestionar el RNBD. Tramitar consultas y reclamos complejos.	A través de planes de trabajo, auditorías, seguimiento a indicadores, elaboración de informes, coordinación inter-áreas,	Continuo. Según plazos legales (Consultas). Anual



	Promover capacitación. Asesorar a las áreas. Realizar evaluaciones de impacto. Gestionar incidentes de seguridad.	desarrollo de material de capacitación, uso de herramientas de gestión.	(Informes, Planes).
Jefes de Área / Líderes de Proceso	Asegurar que los procesos a su cargo cumplan con la Política. Identificar los datos personales tratados en su área. Garantizar que el personal a cargo conozca y aplique la política. Implementar controles específicos del área. Reportar incidentes al OPD.	Mediante la revisión de procesos, listas de chequeo, supervisión del personal, solicitud de asesoría al OPD, aplicación de procedimientos internos.	Continuo. En diseño/modificación de procesos.
Unidad de Informática	Implementar y mantener las medidas de seguridad técnicas (controles de acceso, cifrado, backups, etc.). Apoyar al Oficial de seguridad de la Información en investigaciones de incidentes. Asegurar la seguridad en sistemas de información.	Siguiendo políticas de seguridad de la información, aplicando estándares técnicos, realizando monitoreo, gestionando permisos de usuario.	Continuo. Según plan de mantenimiento y seguridad.
Oficina Asesora Jurídica	Brindar asesoría legal en la interpretación y aplicación de la normativa. Revisar contratos con Encargados. Apoyar en la gestión de requerimientos legales y de la SIC. Revisar la política y sus actualizaciones.	Mediante conceptos jurídicos, revisión documental, acompañamiento en procesos legales.	A requerimiento. En actualizaciones de política.
Unidad de Talento Humano	Incluir obligaciones de protección de datos en contratos laborales. Incorporar la capacitación en protección de datos en la inducción y reinducción. Gestionar los datos de empleados conforme a la política.	Mediante cláusulas contractuales, programas de capacitación, aplicación de procedimientos de gestión de personal.	En contratación. Anual (Capacitación). Continuo.
Oficina de Atención al Usuario / Canales PQRSDF	Ser el primer punto de contacto para recibir consultas y reclamos de los titulares. Orientar a los Titulares sobre el procedimiento. Escalar casos complejos al Oficial de seguridad de la información. Registrar las solicitudes.	Siguiendo el procedimiento establecido en esta Política, utilizando los sistemas de registro de PQRSDF.	Diario / A demanda del Titular.
Todo el Personal (Funcionarios, Contratistas, etc.)	Conocer y cumplir la Política. Tratar los datos personales únicamente para las finalidades autorizadas. Mantener la confidencialidad. Reportar cualquier incidente o sospecha de violación de seguridad al jefe inmediato o al Oficial de	Mediante la lectura y aplicación de la política, el uso responsable de sistemas y datos, la comunicación oportuna de incidentes, la asistencia a capacitaciones.	Continuo / Diario.



	seguridad de la información. Participar en las capacitaciones.		
Todo el Personal (Funcionarios, Contratistas, etc.)	Conocer y cumplir la Política. Tratar los datos personales únicamente para las finalidades autorizadas. Mantener la confidencialidad. Reportar cualquier incidente o sospecha de violación de seguridad al jefe inmediato o al Oficial de seguridad de la información. Participar en las capacitaciones.	Mediante la lectura y aplicación de la política, el uso responsable de sistemas y datos, la comunicación oportuna de incidentes, la asistencia a capacitaciones.	Continuo / Diario.

● 9. IMPLEMENTACIÓN

La implementación efectiva de esta Política contribuye directamente al desarrollo de procedimientos específicos para cada etapa del ciclo de vida de los datos personales, incluyendo:

- **Recolección de Datos Personales:** Se asegurará el método y los medios de recolección de datos personales, obteniendo el consentimiento del titular cuando se requiera y garantizando que los datos recopilados sean pertinentes y apropiados para el propósito comunicado.
- Implementar formularios web seguros (HTTPS) y controles de entrada para prevenir inyecciones SQL y otros ataques.
- Implementar controles de acceso basados en roles para limitar quién puede acceder a qué datos.
- Realizar copias de seguridad periódicas y pruebas de restauración.
- Utilizar firewalls y sistemas de detección de intrusiones.
- Asegurar que las políticas de uso de datos estén documentadas y sean comunicadas a todo el personal.
- Establecer procedimientos para la transferencia de datos a terceros, incluyendo acuerdos de confidencialidad con los Encargados del Tratamiento.
- **Almacenamiento de Datos Personales:** Se garantizarán los mecanismos seguros para el almacenamiento de los datos personales, tanto en formato físico como electrónico, garantizando su confidencialidad e integridad. Se definirá el tiempo de conservación de los datos de acuerdo con la finalidad del tratamiento y la normativa aplicable.
- **Uso de Datos Personales:** El uso de los datos personales se limitará a las finalidades informadas al Titular y autorizadas por este o por la ley.



- **Circulación de Datos Personales:** La circulación de datos personales a terceros sólo se realizará con la autorización del Titular o en los casos permitidos por la ley. Se establecerán acuerdos de confidencialidad con los Encargados del Tratamiento.
- **Transferencia y Transmisión Internacional de Datos Personales:** En caso de ser necesaria la transferencia o transmisión internacional de datos personales, se cumplirán los requisitos establecidos en la legislación Colombiana. Se obtendrá la autorización de la Superintendencia de Industria y Comercio cuando sea requerida.

- **10. SEGUIMIENTO**

El seguimiento al cumplimiento y efectividad de esta Política se realizará de manera continua y periódica como a continuación se detalla.

SEGUIMIENTO DE CUMPLIMIENTO DE INDICADOR Y CRONOGRAMA PROPUESTO: el Área de Gestión de Calidad realiza el monitoreo semestral del indicador y la ejecución del cronograma propuesto.

- **INDICADOR**

NOMBRE INDICADOR	DETALLE	FÓRMULA	PERIODICIDAD
Mitigación de Amenazas Cibernéticas	Resolución de las amenazas cibernéticas reportadas por medio de la mesa de servicio del Hospital Militar Central .	(Total de casos solucionados / Número de casos reportados sobre amenazas cibernéticas (credenciales - Phishing- malware) * 100	Semestral

Este seguimiento se alinearé con las estrategias y metodologías de mejora continua y gestión de calidad implementadas en el Hospital Militar Central.

- **CRONOGRAMA DE ACTIVIDADES (ANUAL)**

A continuación, se establece el siguiente cronograma de trabajo, en el cual se establecen las acciones para llevar a cabo la implementación de la Política de Protección de Datos Personales del Hospital Militar Central, durante la vigencia 2025 – 2027:



Ítem	Actividades	Responsables	Vigencia / Semestre
1	Gobernanza y Marco Normativo		
1.1	Aprobar la Política de Protección de Datos y sus actualizaciones.	Dirección General	2025 S2 (Continuo al emitir/actualizar política)
1.2	Proveer los recursos necesarios para la implementación de la política.	Dirección General	2025 S2 (Continuo al emitir/actualizar política)
1.3	Brindar asesoría legal en la interpretación y aplicación de la normativa; Revisar la política y sus actualizaciones; Revisar contratos con Encargados del Tratamiento.	Oficina Asesora Jurídica	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2027 S2 (A requerimiento, en actualizaciones de política)
2	Implementación Operativa y de Seguridad		
2.1	Liderar, supervisar y coordinar la implementación y cumplimiento de la Política.	Oficial de Seguridad / o quien haga sus veces	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2027 S2 (Continuo)
2.2	verificar cumplimiento normativo del registro Nacional de Bases de Datos – RNBD	Oficial de Seguridad / o quien haga sus veces	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2027 S2 (Continuo)
2.3	Asegurar que los procesos a cargo de cada área cumplan con la Política; Identificar los datos personales tratados en su área; Implementar controles específicos del área.	Jefes de Área / Líderes de Proceso	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2027 S2 (Continuo, en diseño/modificación de procesos)



2.4	Implementar y mantener las medidas de seguridad técnicas (controles de acceso, cifrado, backups, firewalls, detección de intrusiones); Asegurar la seguridad en sistemas de información; Apoyar en investigaciones de incidentes.	Unidad de Informática	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2027 S2 (Continuo, según plan de mantenimiento y seguridad)
2.5	Incluir obligaciones de protección de datos firma de acuerdos de confidencialidad en contratos laborales o con empresas; Gestionar los datos de empleados conforme a la política.	unidad de Talento Humano - área de gestión de contratos	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2027 S2 (En contratación, Continuo)
3	Fomento de la Cultura y Concienciación		
3.1	Promover una cultura de protección de datos desde el más alto nivel.	Dirección General	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2027 S2 (Continuo)
3.2	Promover capacitación; Incorporar la capacitación en protección de datos en la inducción y reinducción; Participar en las capacitaciones.	Oficial de Seguridad / o quien haga sus veces, Unidad de Talento Humano, unidad de contratos, Todo el Personal	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2027 S2 (Anual - Capacitación, Continuo)
4	Atención al Titular y Gestión de Incidentes		
4.1	Ser el primer punto de contacto para recibir consultas y reclamos de los Titulares; Registrar las solicitudes.	Oficina de Atención al Usuario / Canales PQRSDF, mesa de servicio UNIN	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2027 S2 (Diario / A demanda del Titular)
4.2	Orientar a los Titulares sobre el procedimiento; Escalar casos complejos al Oficial de Seguridad de la Información / Área Designada.	Oficina de Atención al Usuario / Canales PQRSDF / mesa de servicio UNIN	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2027 S2 (Diario / A demanda del Titular)



4.3	Tramitar consultas y reclamos complejos relacionados con protección de datos.	Oficial de Seguridad / o quien haga sus veces	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2027 S2 (Según plazos legales, Continuo)
4.4	Gestionar incidentes de ciberseguridad que se puedan presentar.	Oficial de Seguridad / o quien haga sus veces.	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2027 S2 (Continuo / Diario)
5	Seguimiento y Mejora Continua		
5.1	Resolución de las amenazas cibernéticas reportadas por medio de la mesa de servicio del Hospital Militar Central.	Oficial de Seguridad / o quien haga sus veces	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2027 S2 (Semestral)
5.2	Informe sobre los incidentes reportados.	Oficial de Seguridad / o quien haga sus veces	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2027 S2 (Continuo)
5.3	Realizar seguimiento a los indicadores.	Área de gestión de calidad	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2027 S2 (Punto regular en la agenda del comité)
6	Comunicación y Acceso a la Información		
6.1	Publicación permanente de la política en la Intranet y sitio web oficial del Hospital Militar Central	Unidad de Informática	2025 S2, 2026 S1, 2026 S2, 2027 S1, 2

● 12. COMUNICACIÓN Y CONSULTA

La presente Política será comunicada y socializada a todo el personal vinculado, contratistas y terceros relevantes, posterior a la aprobación como corresponde a lo indicado por la normatividad, a través de los siguientes medios:



- Publicación permanente en la Intranet y en la sección correspondiente del sitio web oficial del Hospital Militar Central (www.hospitalmilitar.gov.co).
- Comunicación oficial vía correo electrónico institucional al momento de su expedición y en cada actualización sustancial.
- **Rutas de Consulta del Documento:** El documento oficial y vigente de la Política estará disponible para consulta permanente en:
 - El Sistema de Gestión Documental del Hospital Militar Central (para personal interno).
 - La sección de "Transparencia" o "Protección de Datos" del sitio web oficial del Hospital Militar Central.
 - Se podrá solicitar una copia o información específica a través de los canales de Atención al usuario y relacionamiento ciudadano o contactando al Oficial de seguridad de la Información / Área Designada.

Consulta sobre el Tratamiento de Datos: Los Titulares podrán realizar consultas sobre el tratamiento de sus datos personales o sobre la aplicación de esta política a través de los canales definidos para el ejercicio de sus derechos - Procedimiento para PQRSFD, que incluye correo electrónico, oficina de atención al usuario y relacionamiento ciudadano.

• **13. BIBLIOGRAFÍA**

Colombia. Asamblea Nacional Constituyente. (1991). *Constitución Política de Colombia*. Gaceta Constitucional No. 114.

Colombia. Congreso de la República. (17 de Octubre de 2012). *Ley Estatutaria 1581*. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587.

Colombia. Congreso de la República. (06 de Marzo de 2014). *Ley Estatutaria 1712*. 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. Diario Oficial No. 49.084.

Colombia. Congreso de la República. (31 de Diciembre de 2008). *Ley 1266*. Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales (...). Diario Oficial No. 47.219.

Colombia. Congreso de la República. (04 de Agosto de 2021). *Ley 2126*. Por medio de la cual se modifica parcialmente la Ley 1581 de 2012 (...). Diario Oficial No. 51.756.



Colombia. Ministerio de Comercio, Industria y Turismo. (27 de Junio de 2013). *Decreto 1377*. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial No. 48.835.

Colombia. Ministerio de Comercio, Industria y Turismo. (13 de Mayo de 2014). *Decreto 886*. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos. Diario Oficial No. 49.151.

Colombia. Ministerio de Comercio, Industria y Turismo. (26 de Mayo de 2015). *Decreto 1074*. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Diario Oficial No. 49.523. (Capítulos 25 y 26).

Colombia. Superintendencia de Industria y Comercio. (03 de Noviembre de 2015). *Circular Externa No. 002*. Adiciona el Capítulo Segundo del Título V de la Circular Única de la Superintendencia de Industria y Comercio (Guía Accountability).

[Incluir otras normas relevantes como Resoluciones de Historia Clínica, Políticas internas de SÍ, etc., siguiendo formato APA o ICONTEC].

● 14. ANEXOS

- Acuerdo de confidencialidad empresas Código: **GT-UNIN-PO-02-FT-01**.
- Acuerdo de confidencialidad servidores públicos, contratistas, personal externo Código: **GT-UNIN-PO-02-FT-02**.

● 15. CONTROL DE CAMBIOS

ID	ACTIVIDADES QUE SUFRIERON CAMBIOS	OBSERVACIONES DEL CAMBIO	MOTIVOS DEL CAMBIO	FECHA DEL CAMBIO
001	Resolución N° 1148 (Adopción de la Política)	Inclusión del marco legal (Ley 352/1997, Decreto 1377/2013). -Asignación de responsabilidades de actualización.	Formalizar la adopción de la política y cumplir con lineamientos institucionales.	05/10/2017

Se presentará ante el comité de gestión y desempeño de la dirección como punto en la agenda y posterior aprobación.



APROBACIÓN				
	NOMBRE	CARGO	FECHA	FIRMA
ELABORÓ	ING. Jorge Puerto Gualteros	Ingeniero Especialista Área Gestión de la seguridad y Privacidad de la Información Unidad de Informática	Octubre de 2025	
REVISÓ	CT. Luis Fernando Sierra Joya	oficial de seguridad de la información Hospital Militar Central	Octubre de 2025	
	TC. Eduardo Mendoza Palacio	Jefe de Seguridad y Defensa Unidad de Informática	Octubre de 2025	
	Dr. Juan Ramírez Jaramillo	Jefe de Seguridad y Defensa Oficina asesora Jurídica	Octubre de 2025	
	Dra. Diana Maria Velez Arboleda	Líder Oficina Asesora Dirección	Octubre de 2025	
APROBÓ	Coronel Fernando Díaz Muñeton	Subdirector del Sector Defensa Subdirección Administrativa	Octubre de 2025	
	Mayor General Carlos Alberto Rincón Arango	Director de la Entidad Descentralizada Adscrita al Ministerio de Defensa Hospital Militar Central	Octubre de 2025	
CALIDAD Revisión Metodológica	Mayor. Sildrey Arenas Vesga	Oficial de Comisión Administrativa permanente en la administración pública- Responsables Área de Gestión de Calidad	Octubre de 2025	