PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION

2018 - 2022

TABLA DE CONTENIDO

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION 2018-2022

1. GENERALIDADES

1.1. OBJETIVO

El Plan Estratégico de Tecnologías de la Información para el Hospital Militar Central busca ser la guía tecnológica alineada a la estrategia de tecnología del sector defensa y a los objetivos sectoriales e institucionales para implementar soluciones y servicios de TI en busca de la prestación de servicios de salud.

1.2 OBJETIVOS ESPECIFICOS

- Identificar y alinear los proyectos de TI con los objetivos estratégicos de la entidad para fortalecimiento del entorno y aplicación de TI.
- Realizar una eficiente gestión presupuestal y del gasto público en lo relacionado con la implementación de soluciones de TI.
- Establecer un modelo de gestión de TI mediante el seguimiento de directrices y la implementación de la arquitectura empresarial de TI emitida por el sector defensa.
- Coadyuvar al aprovechamiento estratégico de TI del sector defensa siendo participe en el desarrollo de iniciativas y competencias.
- Implementar al interior de la entidad de la cultura orientada a la calidad de datos y seguridad de la información.

1.3 ALCANCE

Conformar portafolio de proyectos de TI para el lapso 2018-2022 que permitan garantizar una plataforma tecnológica para el Hospital Militar Central dando cumplimiento a los lineamientos que establece la política de gobierno digital, los objetivos y políticas del sector.

2. MARCO NORMATIVO

2.1 OBJETIVO DEL MINISTERIO DE DEFENSA NACIONAL

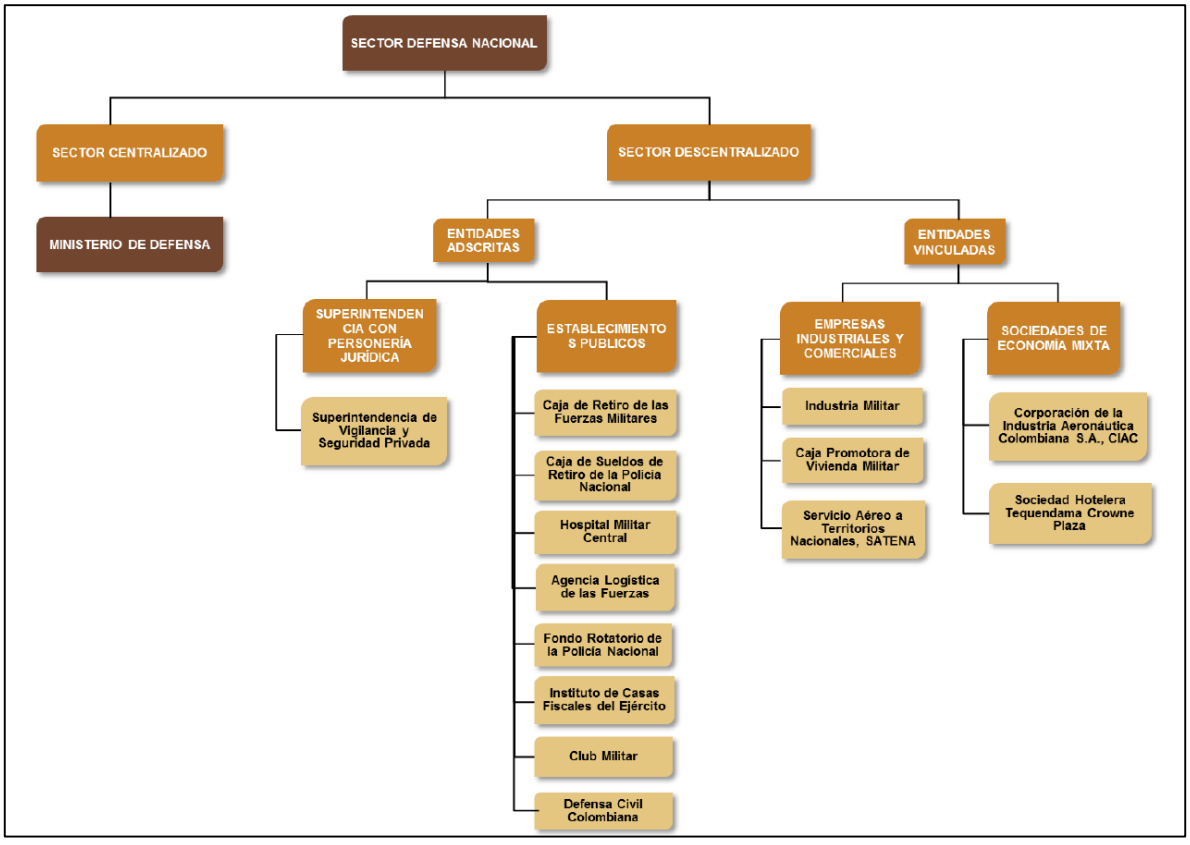
El Ministerio de Defensa Nacional tiene como objetivos primordiales la formulación y adopción de las políticas, planes generales, programas y proyectos del Sector Administrativo Defensa Nacional, para la defensa de la soberanía, la independencia y la integridad territorial, así como para el mantenimiento del orden constitucional y la garantía de la convivencia democrática.

2.2 POLÍTICA DE DEFENSA Y SEGURIDAD

El Objetivo General de la Política de Defensa y Seguridad es coadyuvar a la terminación del conflicto armado, la consolidación de la paz, el desarrollo socioeconómico, la defensa de los intereses nacionales y el mejoramiento de la seguridad pública y ciudadana, mediante el mantenimiento de una Fuerza Pública moderna, fortalecida, motivada y operativa.

2.3 ESTRUCTURA DEL SECTOR DEFENSA

De acuerdo al Manual de Estructura del Estado Colombiano- Sector Defensa – Función Pública, la estructura general del Ministerio de Defensa está establecida en dos grandes sectores: Centralizado y Descentralizado. El Hospital Militar Central se enmarca en la conformación del sector descentralizado como se observa a continuación.



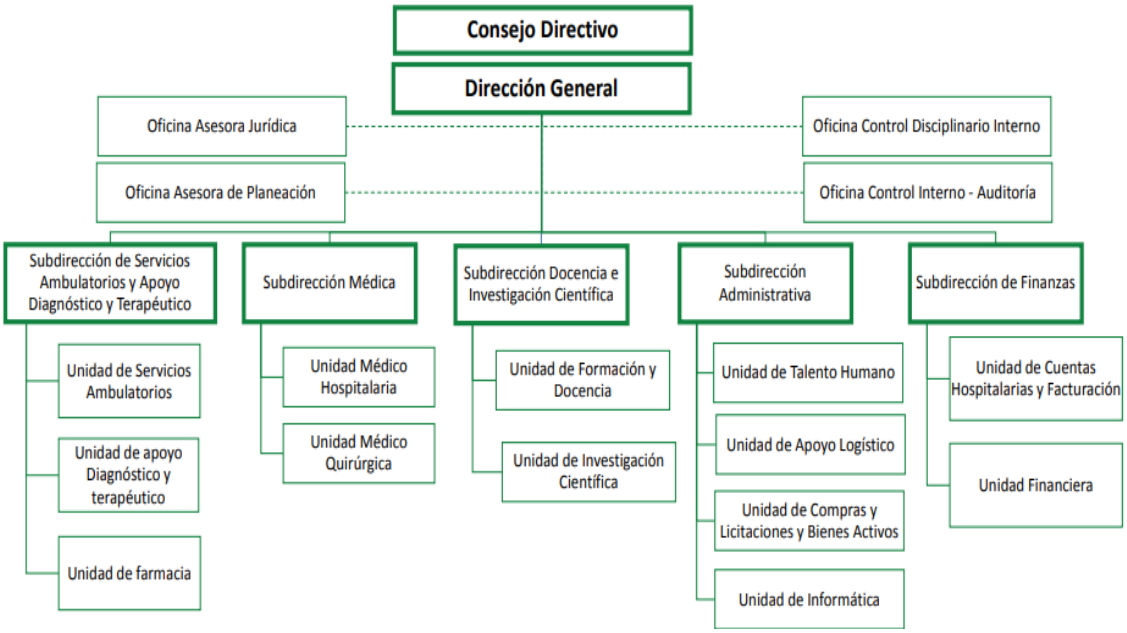
Estructura del Sector Defensa Nacional – Sector Descentralizado

Fuente: Grupo TIC – MDN. Adaptado de Manual de Estructura del Estado, DAFP

En el Ministerio de Defensa Nacional se cuenta con un Grupo de Tecnologías de la Información y Comunicaciones (TIC), creado mediante la Resolución 1374 del 14 de marzo de 2012 como una unidad de trabajo de la Subdirección de Logística y TIC del MDN, cuyas funciones se normaron en el año 2014 y son:

1. Proponer las directrices que definan el direccionamiento de lo relacionado con las tecnologías de la Información y las comunicaciones - TIC, en el sector Defensa.
2. Proponer y estructurar el Plan Estratégico de Tecnologías de Información del sector Defensa.
3. Coordinar la adopción e Implementación de las políticas y directrices que, sobre tecnologías de la Información y las comunicaciones - TIC, emita el Gobierno Nacional.
4. Liderar la adopción de estándares de tecnologías de la Información y las comunicaciones - TIC, en el Sector Defensa.
5. Asesorar a las dependencias y entidades del Sector Defensa en la adopción e implementación de tecnologías de la Información y las comunicaciones - TIC.
6. Proponer Iniciativas de consolidación y capacitación tecnológica en el Sector Defensa.

El Hospital Militar Central cuenta con una Unidad de Informatica, dependiente de la subdirección administrativa, cuyo objetivo principal es “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.”.



Internamente la unidad de informática del Hospital Militar Central se encuentra organizada en cuatro áreas que desarrollan todas las actividades en cumplimiento al cubrimiento de la prestación de servicios informáticos así:

- Gestión de seguridad informática
- Gestión de Infraestructura y Comunicaciones
- Gestión de Aplicaciones, Movilidad y Optimización
- Gestión de Respuesta a requerimientos e incidentes

2.4 NORMATIVIDAD

Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 594 de 2000.	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
Decreto 1747 de 2000.	Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con: "Las entidades de certificación, los certificados y las firmas digitales".
Ley 962 de 2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos Administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones.
Decreto 4890 de 2011	Por el cual se modifica parcialmente la estructura del Ministerio de Defensa Nacional y Se dictan otras disposiciones.
Decreto 19 de 2012	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Resolución 1374 de 2012	Por la cual se adiciona la resolución 127 de 2012 "Por la cual se crean y organizan Grupos Internos de Trabajo del Ministerio de Defensa Nacional".
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
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.
Resolución 10584 de 2014	Por la cual se modifica parcialmente la resolución 1374 de 2012, - para ajustar las funciones del Grupo de Tecnología de Información y las Comunicaciones TIC.
Ley 1753 de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014 - 2018.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1078 de 2015	Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y las comunicaciones – Título 9 – Capítulo I.
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del Sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

3. RUPTURA ESTRATEGICA

Para el Ministerio de Defensa las rupturas identificadas proponen un cambio en el enfoque estratégico, de tal forma que permita transformar, innovar, adoptar un modelo y permitir que la tecnología se vuelva un instrumento que genera valor.

En ese sentido, el Plan Estratégico Sectorial de TI busca ser una herramienta que permita fortalecer las capacidades del Sector en materia de TIC[1]. Por lo tanto, para llevar a cabo la transformación de la gestión de TI y el logro de resultados de impacto en el desarrollo de las actividades del Sector Defensa, se definieron las premisas descritas en la tabla 1, enmarcadas en cada uno de los componentes del DOMPI[2] (Doctrina, Organización, Material y Equipo, Personal e Infraestructura), los cuales se definen a continuación:

[1] El Sector trabaja en la implementación del Modelo de Planeación y Desarrollo de las Capacidades de la Fuerza Pública, el cual se define como el conjunto de procesos, instancias, responsables y productos, que, de manera articulada y continua, traducen los lineamientos políticos y las prioridades estratégicas de defensa y seguridad, en las capacidades requeridas para la proyección y desarrollo de una estructura de fuerza flexible, adaptable y sostenible de mediano y largo plazo.

[2] Se entiende por capacidad, la habilidad de una unidad militar, policial o de la DIMAR de realizar una tarea, bajo ciertos estándares (como tiempo, distancia, simultaneidad, etc.), a través de la combinación de sus respectivos componentes: (i) Doctrina y documentos

Doctrina y documentos que soportan la capacidad: conjunto de saberes, principios, instrucciones, enseñanzas y normas, que guían los procesos y procedimientos para el cumplimiento de la misión constitucional de las Fuerzas Militares, la Policía Nacional y la DIMAR, en aspectos operativos, administrativos y organizacionales.

Organización: estructura funcional y espacial de las unidades, mediante la cual los componentes (Personal, Infraestructura y Material-Equipo) de las Fuerzas Militares, la Policía Nacional y la DIMAR, interactúan coordinadamente para lograr su misión. Este componente incluye funciones, estructura, protocolo organizacional, mando, coordinación y comunicación.

Material y Equipo: corresponde a los elementos necesarios para desarrollar, mantener y sostener las actividades encaminadas al cumplimiento de la misión constitucional. ***Material:*** comprende los elementos de consumo (insumos, repuestos y accesorios). ***Equipo:*** elementos devolutivos que intervienen en el desarrollo de las actividades encaminadas a la consecución de las tareas asignadas.

Personal: conjunto de individuos uniformados y civiles requeridos para el cumplimiento de las tareas asignadas. Este componente contempla el liderazgo individual y el ciclo de vida de los individuos el cual está compuesto por incorporación, formación, capacitación, desarrollo y retiro, incluyendo beneficios, salarios, pensiones, entre otros.

Infraestructura: corresponde al conjunto de bienes inmuebles, redes de servicios e instalaciones necesarios para el desarrollo de las capacidades asignadas. Este componente incluye infraestructura en propiedad o en tenencia[3]

D	**Doctrina**	- La tecnología debe ser considerada un factor de valor estratégico para el Ministerio de Defensa Nacional, sus Unidades Ejecutoras, la Policía Nacional y sus entidades adscritas y vinculadas. - Definir y establecer estándares y directrices sectoriales que permitan una eficaz y eficiente gestión de TI.
O	**Organización**	- La gestión sectorial de TI requiere una gerencia integral que dé resultados. - Adecuar las estructuras organizacionales de acuerdo con sus disponibilidades presupuestales (sin incrementar los gastos de personal) con el fin de garantizar el fortalecimiento institucional y el posicionamiento de las áreas de TI, de manera que dependa del máximo jefe de la respectiva entidad y garantizando su participando en el comité directivo de la misma.

que soportan la capacidad, (ii) Organización, (iii) Material y Equipo, (iv) Personal, e (v) Infraestructura - (DOMPI). Las capacidades se clasifican en operacionales y organizacionales, dentro de estas últimas se ubican las capacidades de TIC.

[3] Propiedad: hace referencia al dominio del bien. Tenencia: Hace referencia al derecho de uso del bien sin título de dominio (comodatos, arriendo, reserva, préstamos, convenios, destinaciones provisionales, entre otros.)

M	 **Material y Equipo**	- Contar con Hardware y Software actualizado de manera que permita que la información cuente con mayor oportunidad, confiabilidad y detalle. - El Sector Defensa debe tener una línea de crecimiento de Hardware y Software armónica y coherente, estableciendo estándares de integración e interoperabilidad.
P	 **Personal**	- Fortalecer el Talento humano de las áreas de tecnología del Sector y desarrollar sus capacidades de uso y apropiación de TIC. - Establecer la figura de Director de Tecnologías y Sistemas de Información Sectorial, quien será el responsable del seguimiento y control de la ejecución de los planes, programas y proyectos de tecnologías y sistemas de información del Sector.
I	 **Infraestructura**	- El Sector Defensa debe contar con las instalaciones físicas que le permitan desarrollar y mantener un centro de datos conjunto, acorde a las necesidades, para apoyar la seguridad y defensa de la Nación.

Tabla 1. Rupturas estratégicas enfocadas en el DOMPI

Tomando como premisa la definición de las rupturas estratégicas realizadas por el Ministerio de Defensa enfocadas en el DOMPI, el Hospital Militar Central en cumplimiento a las directrices emitidas acoge estas definiéndolas para la entidad así:

D	 **Doctrina**	- Adoptar y establecer los estándares y directrices sectoriales a nivel de la entidad que permitan una eficaz y eficiente gestión de TI.
O	 **Organización**	- Adecuar la estructura organizacional de la entidad para que la Unidad de Informática dependa de la dirección de la entidad con el fin de generar fortalecimiento institucional, posicionamiento de las TI

M	 **Material y Equipo**	- Contar con Hardware y Software actualizado de manera que permita que la información cuente con mayor oportunidad, confiabilidad y detalle, estableciendo estándares de interoperabilidad e integración.
P	 **Personal**	- Fortalecer el Talento humano en la Unidad de Informática y desarrollar sus capacidades de uso y apropiación de TIC.
I	 **Infraestructura**	- Contar con instalaciones físicas adecuadas que permitan desarrollar y mantener el centro de datos y la prestación de servicios informáticos a los diferentes usuarios de la entidad.

4. ANÁLISIS DE LA SITUACIÓN ACTUAL

Se toma como punto inicial la descripción de la situación actual de las tecnologías de la información en relación con los dominios del marco de arquitectura empresarial: Estrategia de TI, Gobierno de TI, Gestión de Información, Sistemas de Información, Servicios Tecnológicos, Uso y Apropiación, situación analizada mediante el resultado de encuestas aplicadas a nivel sectorial por el Grupo de tecnologías de la información del Ministerio de Defensa.

4.1 ESTRATEGIA DE TI

La Estrategia TI es una parte integral de la estrategia de una entidad y busca aportar valor al desarrollo sectorial e institucional de las entidades a través de su proyección.

Entendimiento Estratégico (AM.ES.01):. La entidad ha adoptado estrategias de TI que están alineadas con el plan estratégico sectorial y el Plan Estratégico de Tecnología del Sector, soportadas en el marco de arquitectura TI. Sin embargo, no se cuenta con un Plan estratégico de tecnología planteado oficialmente, ni con el componente de arquitectura empresarial en la entidad por lo que este proceso ha presentado dificultades en su planteamiento.

Direccionamiento Estratégico (AM.ES.02): El Hospital Militar Central para este ámbito ha generado políticas de seguridad, acogiendo los estándares que ha emitido en este tema el Ministerio de Defensa. Al igual que las entidades del sector no se cuenta con un plan de comunicaciones de la estrategia de TI y no se tiene conocimiento de las políticas sectoriales en cuanto a TIC, sistemas de información, servicios tecnológicos y del uso y apropiación de los anteriores que permita: gestión de compras conjuntas, gestión de proyectos integrales con las demás entidades del sector.

Implementación de la Estrategia TI (AM.ES.03): La entidad participa activamente en los proyectos que posee componentes de TI y que son propuestos por las diferentes áreas y realiza el seguimiento correspondiente ante el MDN mediante el CITI y ante el DNP en su plataforma SUIP. El control de recursos financieros que inicia con el plan de compras es ejecutado a través de los actores del proceso de gestión contractual como los comités jurídico, económico y técnico. La Unidad de Informática tiene un catálogo de servicios informáticos establecido con sus correspondientes acuerdos de niveles de servicio que cubre toda la entidad.

Seguimiento y Evaluación de la Estrategia de TI (AM.ES.04): Permite conocer el avance de la implementación, así como el nivel de cumplimiento de la Estrategia de TI. En la entidad se cuenta con herramientas de tablero de control para evaluar el cumplimiento de los indicadores planteados para la Unidad de Informatica.

4.2 GOBIERNO DE TI

EL Gobierno de TI es una práctica, orientada a establecer unas estructuras de relación que alinean los procesos de negocio con los procesos, recursos y estrategias de TI y es parte del gobierno corporativo o empresarial. Su dominio busca aportar valor al desarrollo institucional a través de la implementación de esquemas de gobernabilidad de TI, alineados a los procesos y procedimientos de la entidad.

La estructura organizacional de TI para el Hospital Militar se encuentra en cabeza de la Unidad de Informática, con funciones y actividades que intervienen de manera transversal en todos los proyectos de la entidad acordes a los roles de TI y apoya las decisiones a nivel de alta dirección. También se cuentan con procesos que definen a nivel del sistema de gestión de calidad las actividades que realiza la Unidad en la entidad y con indicadores de cumplimiento y manejo de riesgos de TI.

4.3 INFORMACIÓN

Se entiende por información un conjunto de datos organizados y procesados que tienen un significado, relevancia, propósito y contexto. El dominio de información busca aportar valor estratégico a la toma de decisiones a partir de la gestión de la información como un producto y servicio de calidad.

La entidad ha establecido el catálogo básico de información y está desarrollando el procedimiento para las actividades de gestión y planeación de sus componentes. De igual forma, la Unidad de Informática no realiza

desarrollos de software ni aplicaciones, pero si cuenta con algunos esquemas de interoperabilidad, los cuales aplican en menor grado algunos mecanismos de gestión y planeación de aseguramiento, control, inspección y mejoramiento de la calidad de los componentes de información, pero genera los lineamientos para este tratamiento con la subdirección de docencia en su área de investigación e innovación.

4.4 SISTEMAS DE INFORMACIÓN

Este dominio busca describir la situación actual de los sistemas de información. La no existencia de políticas de tecnologías sectoriales también refleja la necesidad de contar con planes y directrices cuya transversalidad sea aplicable en los procesos de adquisición y soporte en los sistemas de información.

El Hospital Militar Central cuenta con un sistema de información transversal que cubre todas las áreas asistenciales, administrativas y financieras, permitiendo la trazabilidad necesaria para el seguimiento de las actividades que se prestan a los usuarios. Su mantenimiento se encuentra tercerizado y garantiza la actualización y funcionalidad del mismo.

Como sistemas de información de apoyo la entidad cuenta con sistemas de gestión documental, sistemas biomédicos, plataformas educativas, mesa de ayuda y componentes ofimáticos que ayudan a la prestación del servicio de salud y al control de actividades, que hacen parte del diccionario y el catalogo de servicios informáticos.

4.5 SERVICIOS TECNOLÓGICOS

La entidad cuenta con un catálogo de servicios tecnológicos actualizado y su correspondiente acuerdo de niveles de servicio, con una mesa de servicios de control propios y un soporte y mantenimiento prestado por un tercero. No cuenta con servicios en la nube, siguiendo los lineamientos emitidos por el ministerio de defensa y teniendo en cuenta el alto costo que se tendría al utilizarlos, costo que superaría el presupuesto asignado a TI en la entidad.

4.6 USO Y APROPIACIÓN

Con respecto a la estrategia de uso y apropiación de TI, la entidad se encuentra en proceso de establecer las actividades para generar la política de gestión de cambio en los proyectos de TI, la cual debe estar alineada con la cultura organizacional. Adicionalmente se encuentra en preparación el plan de formación de TI para los miembros de la Unidad de Informatica de la entidad.

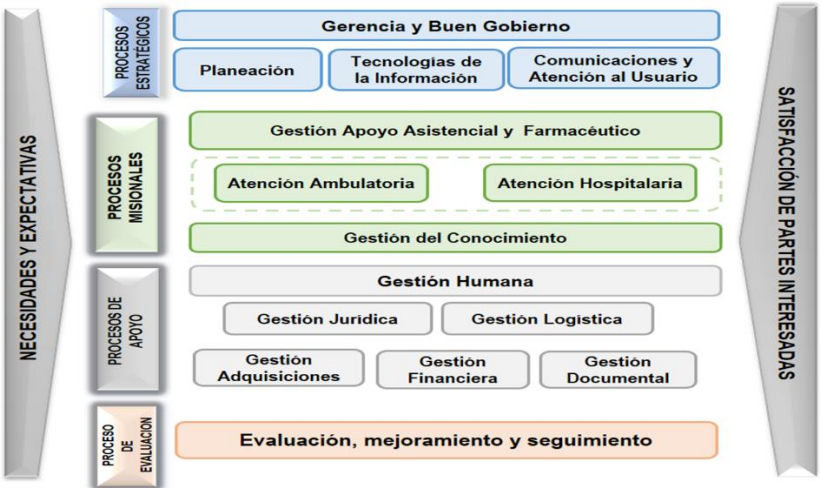
5. ENTENDIMIENTO ESTRATEGICO

5.1 PLAN ESTRATÉGICO DEL SECTOR

El Plan Estratégico del Sector Defensa y Seguridad 2016 - 2018 se construyó bajo los lineamientos del Plan Nacional de Desarrollo (PND) 2014 - 2018 “Todos por un Nuevo País”, la Política de Defensa y Seguridad “Todos por un Nuevo País” y el documento maestro de Transformación y Futuro de la Fuerza Pública - 2030.

Este Plan fue elaborado buscando el cumplimiento de responsabilidades que deben realizarse efectivamente para el cumplimiento de los objetivos planteados en el marco de defensa y seguridad, generando objetivos estratégicos y metas del sector y que son base para formular los planes estratégicos institucionales.

5.2 OBJETIVOS ESTRATEGICOS DE LA ENTIDAD



El Plan Estratégico Sectorial de Tecnologías de Información - PETI, PETI, se enmarca dentro de los procesos estratégicos de la entidad, y al igual que el plan estratégico del sector apoya al cumplimiento del objetivo No 6 del Ministerio de Defensa "*Transformar y Modernizar en forma continua al sector defensa",* Meta 2. " *Implementar modelos que contribuyan a la modernización y sostenibilidad del sector".* El Grupo TIC del Ministerio de Defensa Nacional pertenece al proceso de Tecnologías de Información y Comunicaciones calificado como proceso de apoyo.

A nivel de la entidad se enmarca en el objetivo No 4 "Fortalecer Herramientas que optimicen la atención al paciente", que busca el fortalecimiento de la cobertura en la infraestructura tecnológica.

6.MODELO DE GESTION DE TI

6.1 ESTRATEGIA DE TI

La Estrategia busca que la entidad posea servicios tecnológicos y herramientas para el manejo de la información que ayuden en la optimización de sus procesos, y apoyen la toma de decisiones en pro de garantizar la prestación de servicios de salud a los usuarios de la entidad. De esta forma el Ministerio de defensa nacional ha definido lo siguiente:

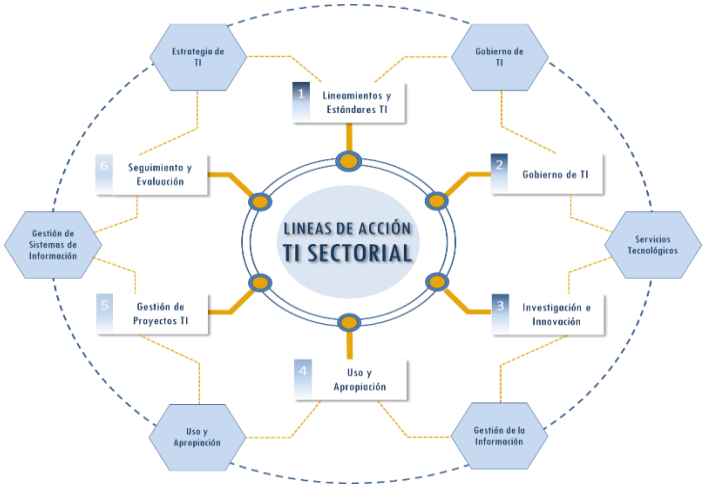
Misión TI Sectorial

"*Establecer directrices que permitan el gobierno y uso apropiado de las TI del Sector, con el fin de facilitar la toma de decisiones adecuadas para la Seguridad y Defensa Nacional, disminuir las brechas de las capacidades operacionales y de soporte y mejorar la interacción con la ciudadanía*".

Visión TI Sectorial

"*Para el 2026 las áreas o dependencias de TI del Sector serán el referente para otros sectores del Gobierno Nacional al tener una gestión adecuada de TI para sus procesos misionales y estratégicos; así mismo, contará con una normatividad de TI para sus procesos tecnológicos; brindará información con altos estándares de calidad al interior y exterior; y contará con interoperabilidad entre sus diferentes plataformas tecnológicas*",

De lo anterior se generan unas líneas de acción sectorial:



Tomando como base lo anterior, para el Hospital Militar Central se plantean las siguientes líneas de acción:

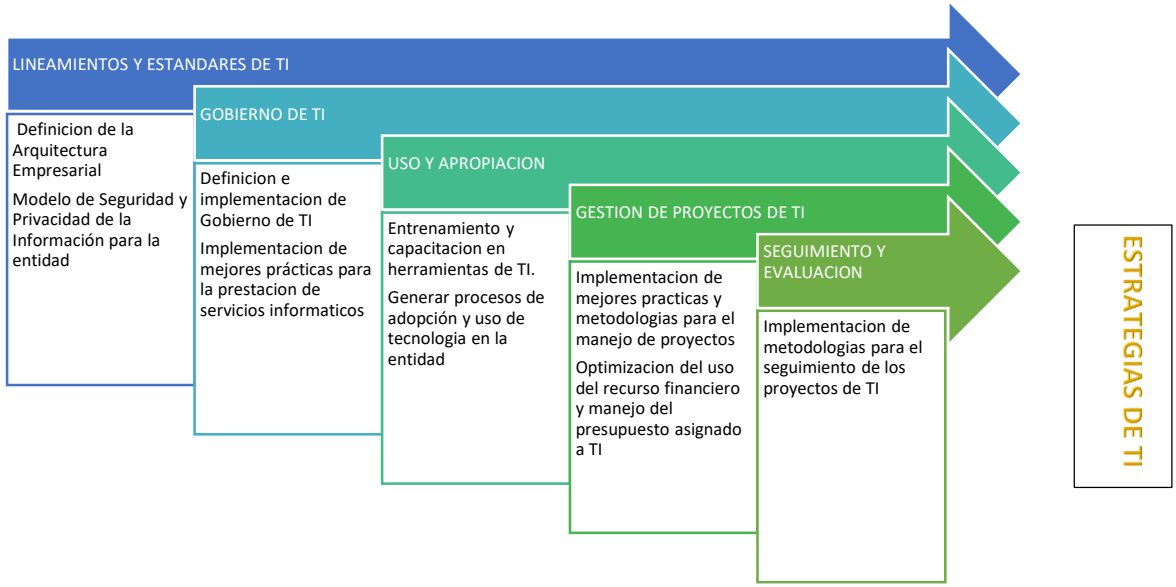
Lineamientos y Estandares de TI	•Adoptar politicas y generar lineamientos para la gestion de TI en la entidad.
Gobierno de TI	•Elaborar e implementar politicas para contar con los niveles adecuados de toma de decisiones a nivel de TI en la entidad.
Uso y Apropiacion	•Generar politicas y directrices para el uso eficiente de soluciones de TI
Gestion de Proyectos	•Adopcion de metodologias y buenas practicas para la adopcion de procesos de TI
Seguimiento y Evaluacion	•Implementacion de indicadores y herramientas de medicion para los proyectos de TI

6.2 Definición de los objetivos estratégicos de TI

A nivel sectorial se determinan cuatro perspectivas estratégicas a nivel de TI y tomando estas como base se establecen los siguientes objetivos estratégicos:

Aporte y valor agregado a las inversiones en TI para el sector defensa.	•Generar proyectos de TI siguiendo los lineamientos del MDN en estandarización de tecnologia e informació, aprovechando al maximo el recurso economico.
Ofrecer servicios efectivos de TI para el sector defensa y la poblacion	•Proveer a la entidad de herramientas y servicios tecnologicos que permitan la prestacion de servicios de salud a la poblacion de manera eficiente y efectiva.
Gestion de Procesos y Proyectos de TI	•Implementar metodologias y buenas practicas para el desarrollo de proyectos de TI en la entidad.
Gestion de Competencias de TI	•Fomentar los procesos de capacitacion y entrenamiento en el personal de TI en las herramientas necesarias para la administracion, seguimiento y evaluacion de las mismas.

6.3 ESTRATEGIAS DE TI



6.4 GOBIERNO DE TI

La estructura de Gobierno de TI que se incorporará en el Sector Defensa tendrá como base COBIT[4], que provee el marco de referencia para alcanzar los objetivos y las funciones de la estructura organizacional que exige el Ministerio TIC a nivel Gobierno y Gestión de las TIC.

Se tendrán en cuenta los siguientes principios:

[4] COBIT: Control Objectives for Information Systems and related Technology – Objetivos de Control para Tecnología de Información y Tecnologías relacionadas.. Es un marco de trabajo enfocado en el gobierno empresarial de las tecnologías de información para que éstas sean gobernadas y gestionadas en forma holística.

- Satisfacer las necesidades del sector en materia de TI, para crear valor en cada una de las unidades ejecutoras, Policía Nacional y entidades adscritas y vinculadas, manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos.
- Cubrimiento de las funciones y procesos transversales de TI a nivel sectorial.
- Aplicar un Marco de Referencia base que pueda ser integrado con diferentes estándares y buenas prácticas.
- Enfoque holístico de un gobierno y gestión de las TI.
- Separar el Gobierno de la Gestión de TI.

6.4.1 Gobierno TIC

El Ministerio de Defensa Nacional emite las políticas, lineamientos y estándares para la adopción e implementación de soluciones tecnológicas para todas las entidades del sector. A nivel del Hospital Militar Central la gobernabilidad de TIC se encuentra bajo la responsabilidad de la Unidad de Informatica quien de manera transversal a los procesos de la entidad busca optimizar las inversiones de TI, gestiona y controla los riesgos y mide el desempeño de TI.

6.4.2 Políticas TIC

La Unidad de Informática del Hospital Militar Central adopta las políticas, lineamientos y estándares relacionados con servicios e infraestructura tecnológica y sistemas de información que genera el Ministerio de Defensa a través de sus viceministerios, y las políticas y lineamientos en ciberdefensa y ciberseguridad que genera el grupo ColCERT.

6.4.3 Aprobación Iniciativas TIC

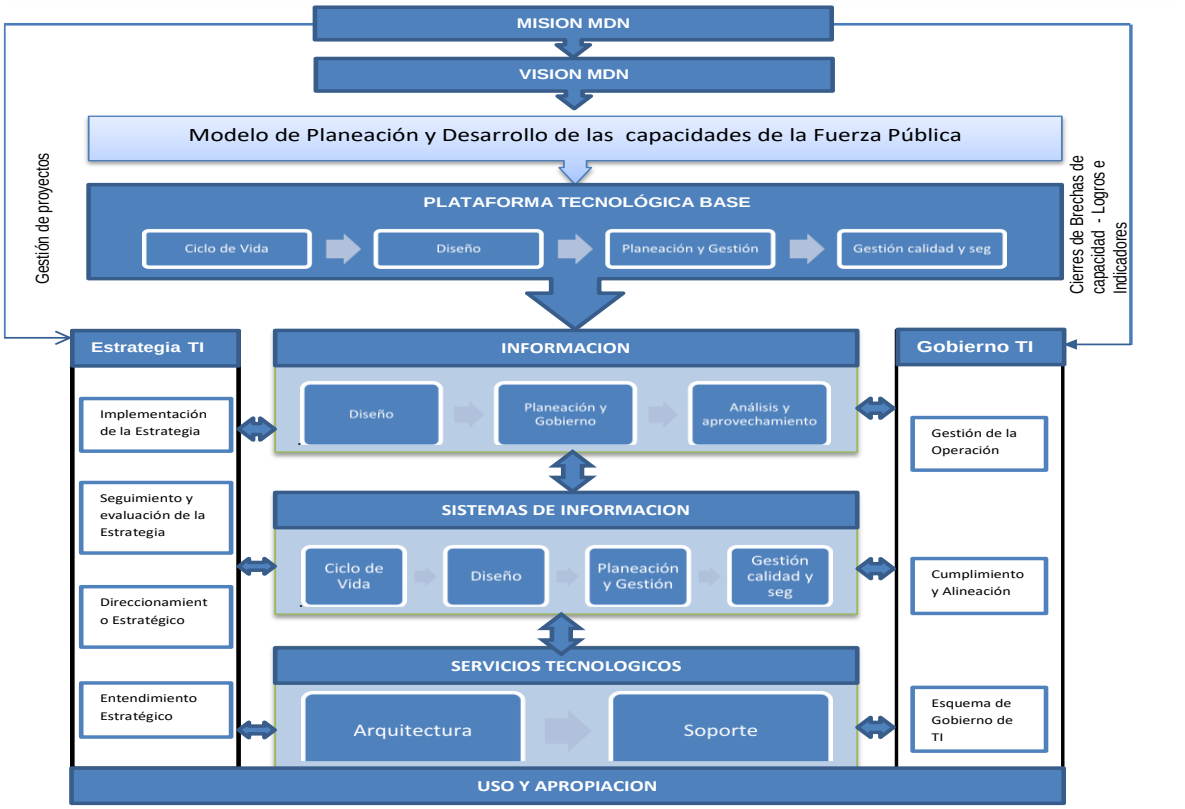
Siguiendo el lineamiento emitido por el Ministerio de Defensa, todo proyecto o iniciativa que se genere en la entidad debe ser presentada ante el Comité de la Integración de Tecnologias de la Informacion y Comunicaciones previa viabilidad del Grupo de las Tecnologías de la Información y Comunicaciones del Ministerio de Defensa, o el que haga sus veces y deben ser inscritos en el Banco de programas y proyectos de inversión nacional BPIN si la fuente de financiación de los mismos corresponda a un recurso de inversión.

6.4.4 Seguimiento y Evaluación TIC

A través de las herramientas establecidas por el Ministerio de Defensa, la Unidad de Informatica de la entidad realiza el seguimiento y evaluación de los proyectos TIC, actividades que son controladas por la Oficina asesora de planeación y estas actividades se realizan basadas en criterios de impacto, efectividad y mejoras de procesos.

6.4.5Cadena de valor de TI

El Hospital Militar Central adopta la cadena de valor de TI que propone el Ministerio de Defensa Nacional asi:



6.5 INDICADORES Y RIESGOS

De acuerdo a la metodología indicada por el Ministerio de Defensa, el Hospital Militar Central utilizará los siguientes indicadores de gestión:

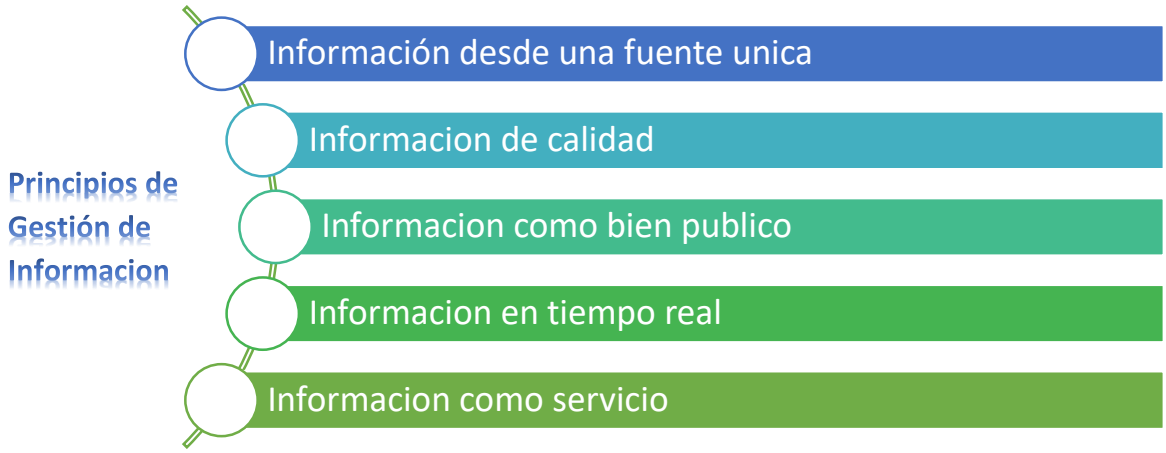
Nombre	Descripción
Nivel de ejecución del Plan de Estratégico de TI	Medirá el avance en la ejecución de los proyectos y actividades del plan estratégico de TI
Disponibilidad de información en medios de T.I.	Uso efectivo de los sistemas y servicios de información de la entidad
Nivel de requerimientos de desarrollo y mantenimiento implementados	Medir el avance en el desarrollo de los requerimientos y el mantenimiento de los sistemas de información con respecto a las necesidades de la arquitectura institucional
Oportunidad en la solución a novedades de la plataforma tecnológica	Medir la oportunidad en la solución de novedades para mantener el uso de los sistemas de información con base en la plataforma tecnológica

En lo relacionado a riesgos, la Unidad de Informática de la entidad propone los siguientes:

No	RIESGO	DESCRIPCION	CAUSAS	CONSECUENCIAS
1	Interrupción en prestación de servicios de TI	No acceso por parte de los usuarios a los servicios definidos como servicios de TI en la entidad. Ej: Dinamica Gerencial, Gestor Documental, etc.	Fallas fisicas o logicas en la infraestructura de TI Falla de monitoreo sobre la operación de la infraestructura TI	1. No disponibilidad de la informacion 2. Afectación en la prestación de servicios de TI al usuario
2	Perdida de los datos almacenados en las bases de datos ubicadas en el datacenter de la entidad	Eliminación de datos que se encuentran en las instancias de las bases de datos que estan almacenadas en el datacenter de la entidad .	Fallas en los equipos de seguridad informatica Insuficiencia en el aseguramiento de la base de datos	1. Incumplimiento normativo 2. Sanciones disciplinarias, administrativas y pnales 3. Perdida del patrimonio documental 4. Reprocesos
3	Afectación de la disponibilidad del respaldo de datos	Realización incompleta o parcial de copias de los datos que están almacenados en las instancias de las bases de datos ubicadas en el datacenter de la entidad.	Fallas en el appliance de backup	1. Fallas en integridad de datos 2. Posible perdida de informacion
4	Inadecuado funcionamiento de las opciones del sistema de informacion	Procesos y procedimientos implementados en el sistema de informacion por parte del propietario del codigo fuente que no funcionan de manera adecuada dentro del sistema de informacion	Fallas en el funcionamiento de las opciones de los modulos en nuevas versiones de actualizacion del sistema de informacion	1. Indisponibilidad de datos para el servicio al usuario

6.6 GESTIÓN DE INFORMACIÓN

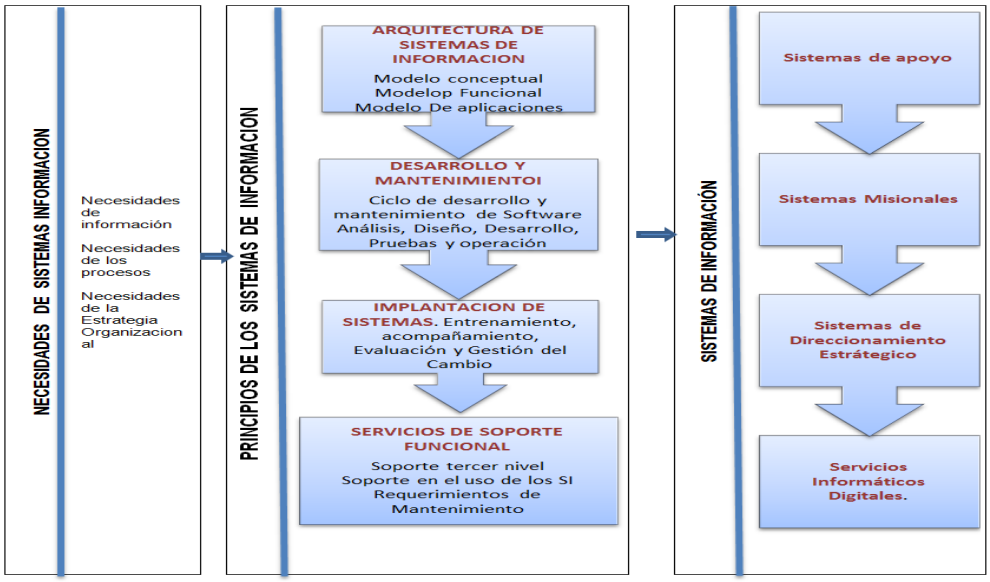
El Modelo de Gestión de TI que se plantea corresponde al indicado para ser adoptado al interior de las entidades del sector defensa, el cual tiene como objetivo establecer los requerimientos de información, actualización de bases de datos y verificación de estas para la consolidación de información.



Como parte de la política de gobierno digital, la unidad de informática se encuentra desarrollando actividades para generar el gobierno de datos al interior de la entidad, aplicando los principios de gestión de información.

6.7 SISTEMAS DE INFORMACIÓN

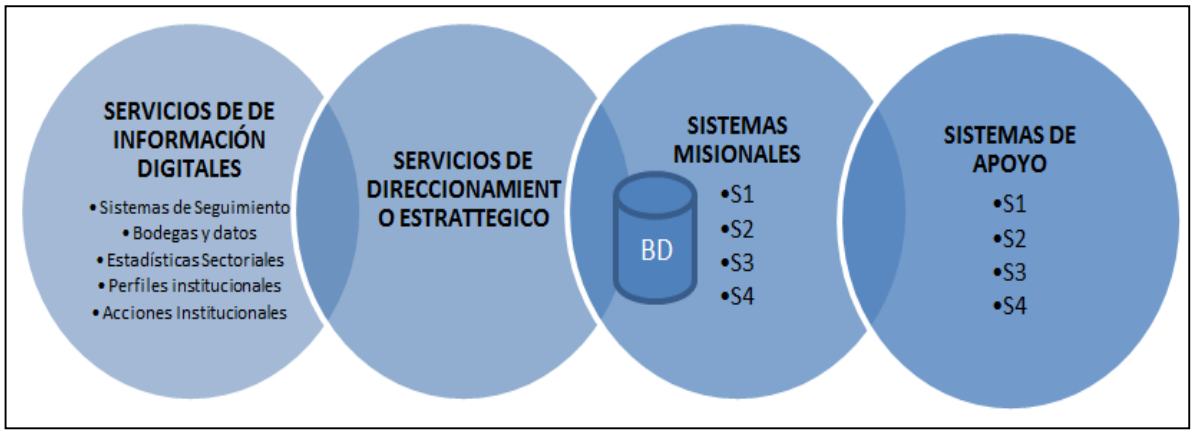
El Hospital Militar Central contará con un sistema de información que cubriría todas las áreas asistenciales, administrativas y financieras consolidándose en una fuente única de datos para la toma de decisiones que realizaría interoperabilidad con el software asistencial de los equipos biomédicos de la entidad. Como modelo de gestión de Sistemas de Información adopta el sugerido por el Ministerio de Defensa así:



Modelo de Gestión de Sistemas de Información

Fuente: Grupo TIC – MDN. Adaptado de: MINTIC

6.7.1 Arquitectura de sistemas de información



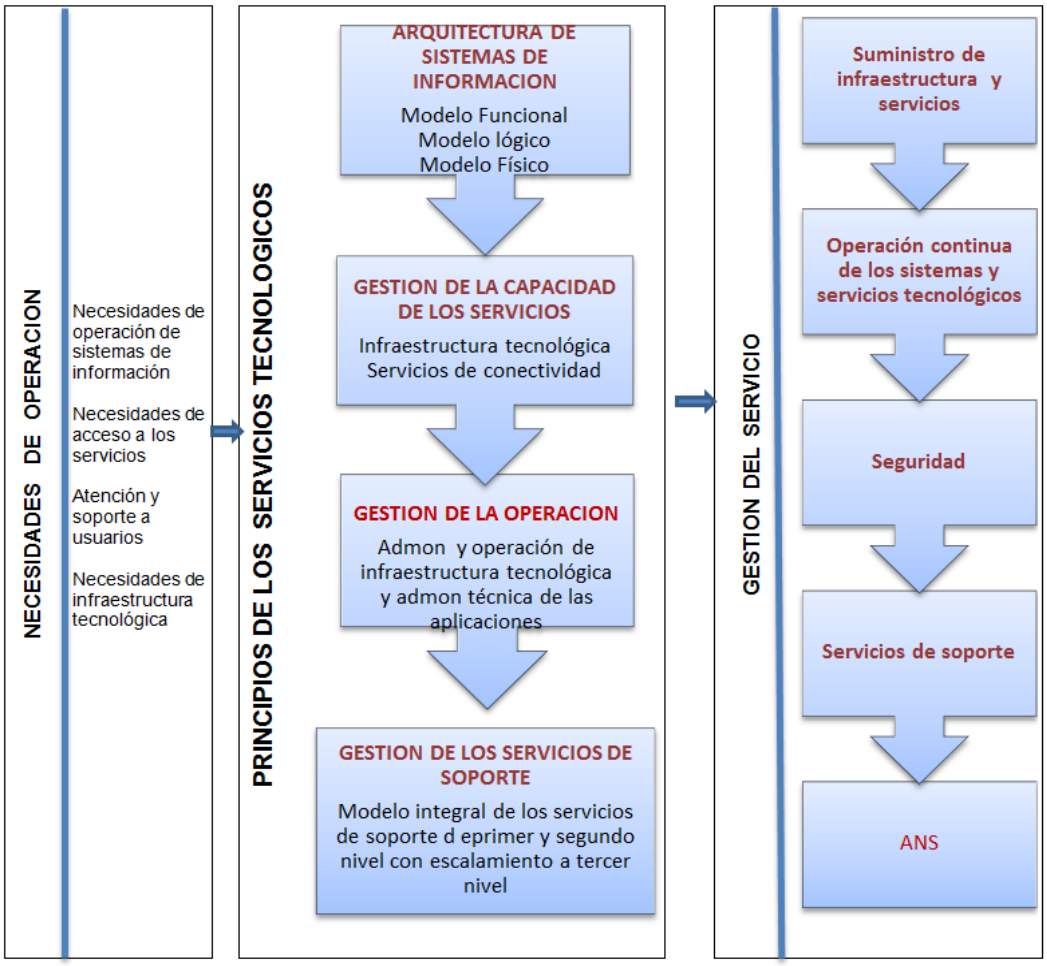
Modelo de Arquitectura de Sistemas de Información

Fuente: Grupo TIC – MDN. Adaptado de: MINTIC

6.7.2 Procedimiento para la implementación de la arquitectura de sistemas de información

6.8 SERVICIOS TECNOLÓGICOS

El Ministerio de Defensa en este punto plantea el siguiente modelo de gestión de servicios tecnológicos que pretende se use tecnologías de información y comunicaciones de vanguardia que contemple la operación continúa, soporte a los usuarios, la administración y el mantenimiento y que implemente las mejores prácticas de gestión de tecnología reconocidas internacionalmente.



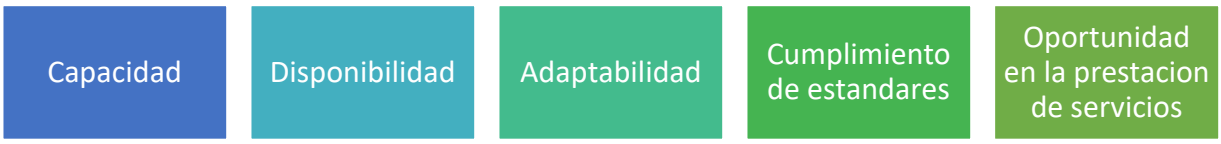
Modelo de Gestión de Servicios Tecnológicos

Fuente: Grupo TIC – MDN. Adaptado de: MINTIC

6.8.1 Criterios de calidad y procesos de gestión de servicios de TIC

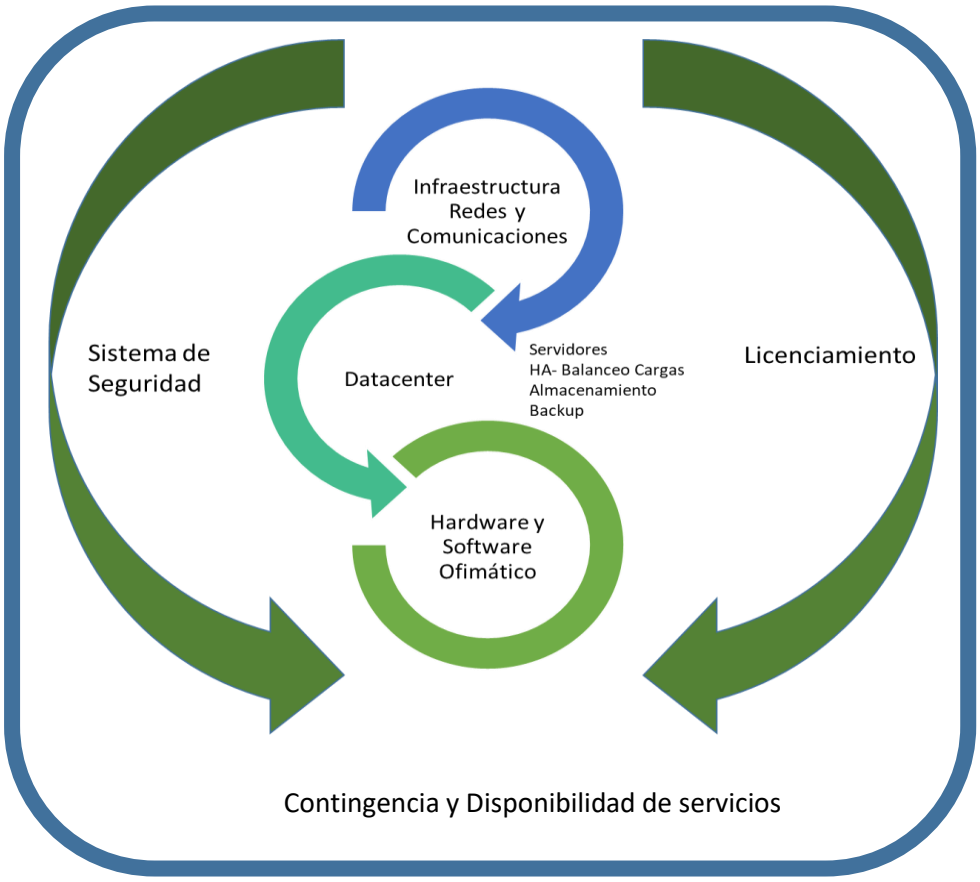
En el Hospital Militar Central adoptará el uso ITIL como mejor práctica para definir los criterios de calidad que garantizan la operación de toda la plataforma tecnológica y de servicios informáticos.

6.8.2 Principios de los servicios tecnológicos



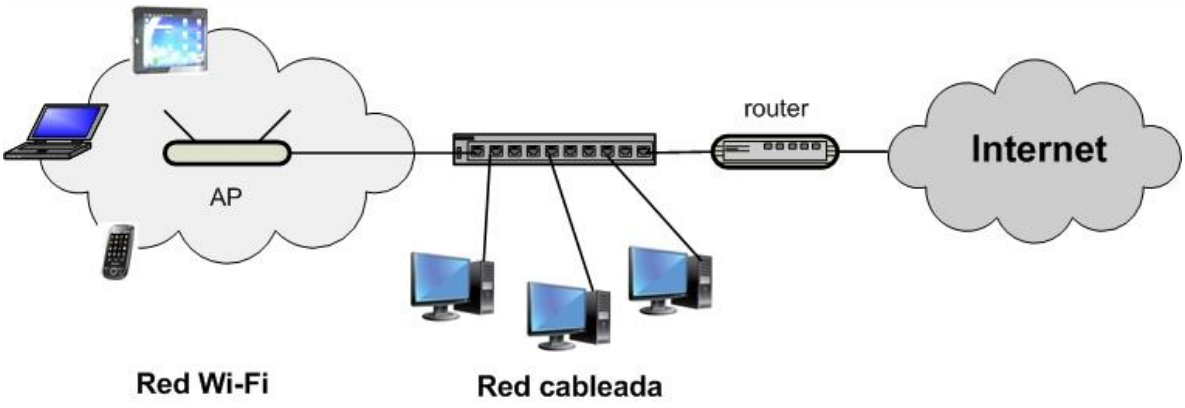
6.9 Infraestructura

El Hospital Militar Central contará con una infraestructura tecnológica que soportará la prestación continua de los servicios informáticos así:



6.10 Conectividad

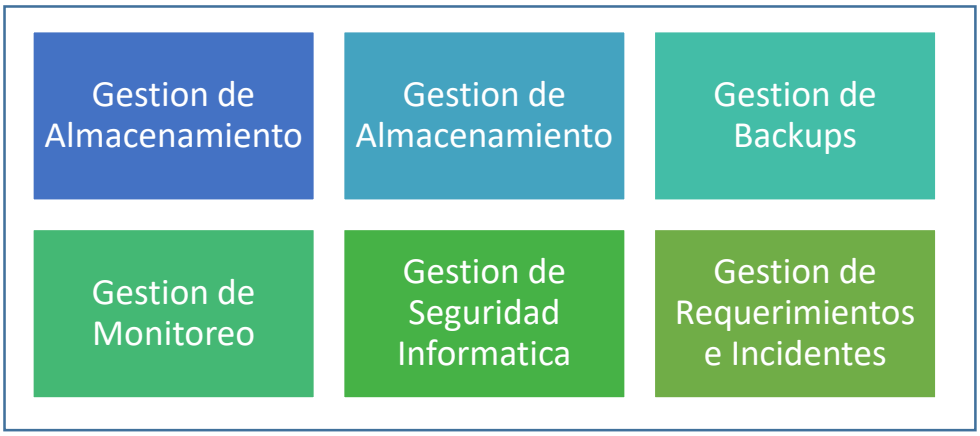
La arquitectura de conectividad propuesta para el Hospital Militar Central corresponde a una red LAN para su sede principal y sus edificios aledaños, con cableado categoría 6 como mínimo, segmentadas en VLAn que se establecerán de acuerdo al servicio asistencial, administrativo o financiero requerido. Sus centros de cableado estarán conectados a 10G con respaldo en fibra. Adicionalmente prestará servicios de redes inalámbricas para cubrimiento de sitios donde la red LAN no puede acceder. El servicio de Wifi se brindará con dos tipos de perfil: un perfil público cuyo acceso correspondería a los usuarios a los que se les presta el servicio de salud y otro privado que se asignaría a personal de la entidad con labores muy específicas que requieren de servicios informáticos especiales, y la prestación de servicios de internet tendrá un canal principal con reuso 1:1 y poseer canal de respaldo activo-activo con garantía de calidad de servicio o QoS.



6.11 Servicios de operación

La entidad garantiza la administración, mantenimiento y soporte del sistema de información mediante contrato de mantenimiento y soporte tercerizado, así como a nivel de la infraestructura de hardware y software ofimático, para los dos casos se utiliza la mesa de ayuda implementada en la entidad que garantiza la trazabilidad y seguimiento de las políticas establecidas para este fin.

La Unidad de Informática establecerá políticas para el manejo de servicios de operación, las más importantes serán:



6.12 Administración De Bases De Datos

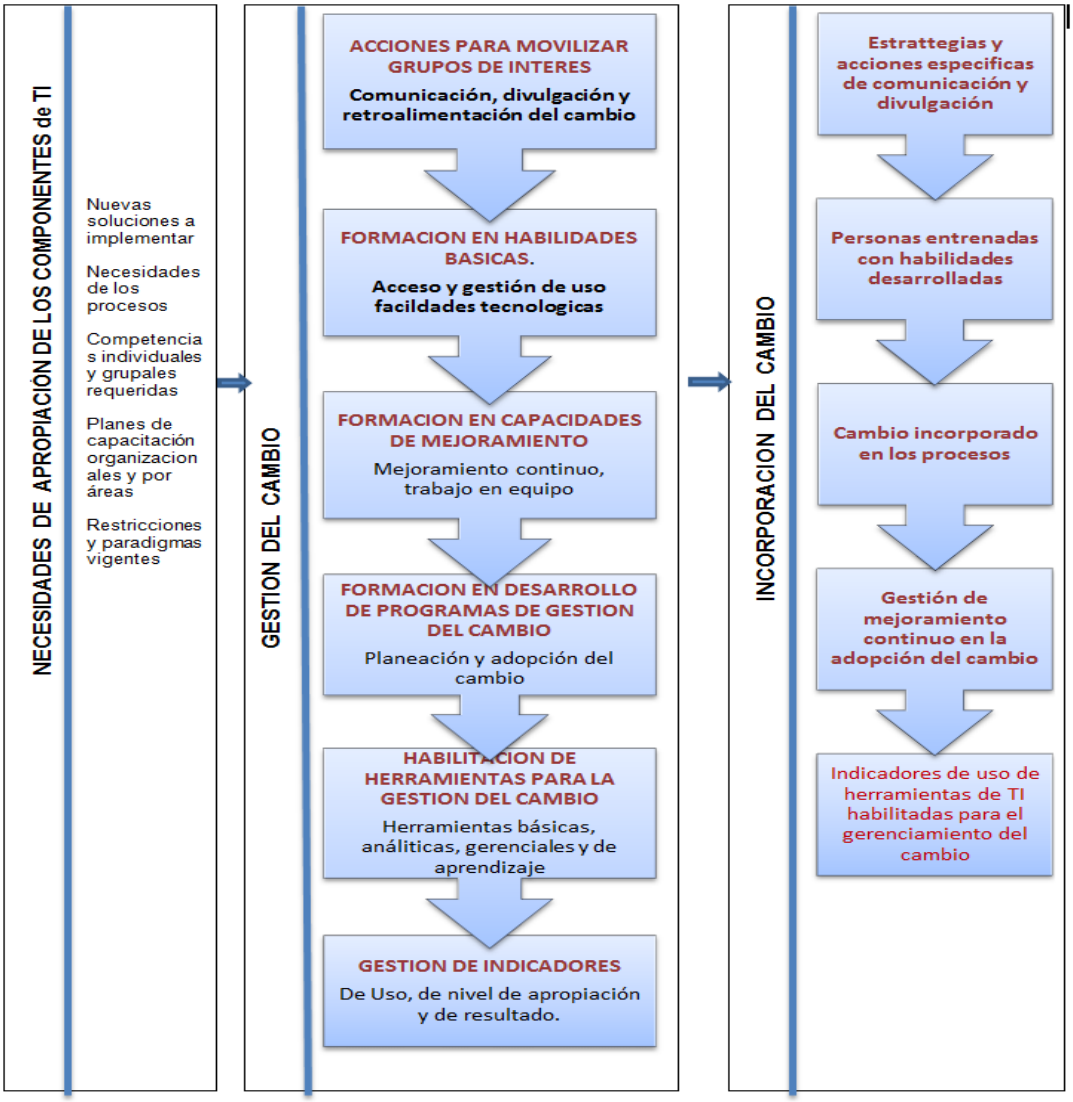
La Unidad de Informática del Hospital Militar Central contará con un área encargada de la administración de las bases de datos Oracle y SQL Server que se tengan implementadas en la entidad, ejecutará las funciones básicas y especializadas para la administración de este tipo de sistemas de gestión.

6.13 Administración De Aplicaciones

Esta área en la entidad se encargará de la administración de los componentes de capa media bajo los cuales correrán las aplicaciones, así como las labores destinadas a la generación de estadísticas de uso y acceso y utilización de herramientas adicionales de software entre otras.

7. USO Y APROPIACIÓN

El Hospital Militar Central adopta el modelo de gestión de uso y apropiación emitido por el Ministerio de Defensa, a nivel de las actividades que debe desarrollar la Unidad de Informática se enfoca en alinear a los funcionarios de la entidad con la estructura de soporte tecnológico de tal manera que se facilite su uso y forme parte de la cultura organizacional del Hospital Militar Central.



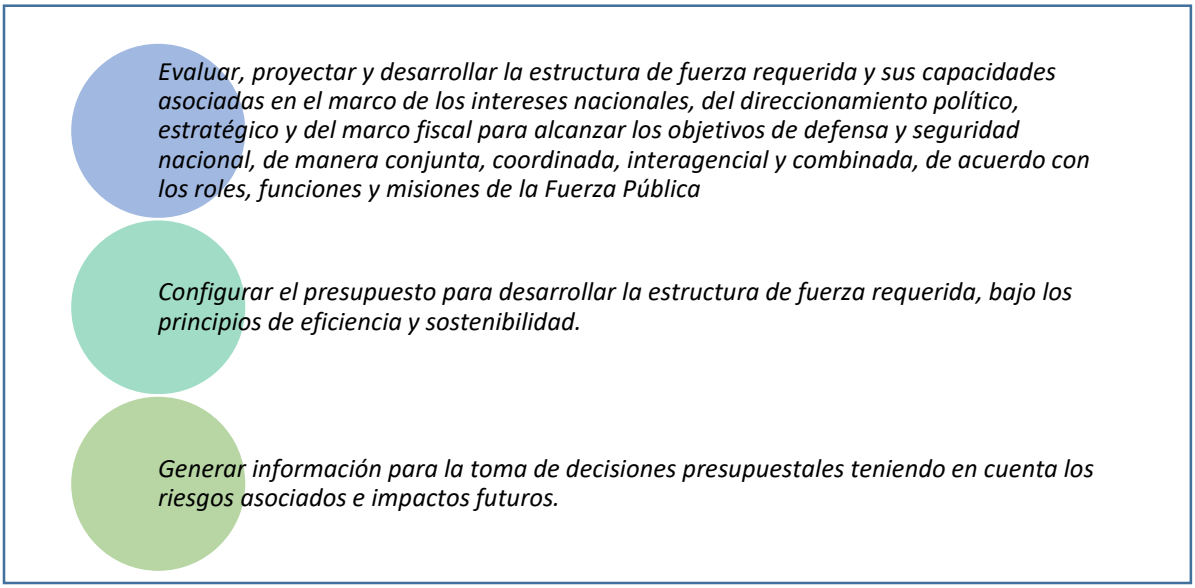
Modelo de Uso y Apropiación de TI

Fuente: Grupo TIC – MDN. Adaptado de: MINTIC

8. MODELO DE PLANEACIÓN

El fortalecimiento institucional del Ministerio de Defensa Nacional ha sido concebido a través de la estrategia de Transformación del Sector Defensa. En tal sentido, desde el año 2012, en conjunto con el Comando General de las Fuerzas Militares, las Fuerzas Militares y la Policía Nacional se han puesto en marcha iniciativas metodológicas para la planeación y programación presupuestal, gestión del capital humano y gestión de la logística del Sector que permita mejorar la planeación de mediano y largo plazo.

Como consecuencia de lo anterior, se creó el Modelo de Planeación y Desarrollo de las Capacidades de la Fuerza Pública, el cual busca cumplir tres objetivos:



De acuerdo a lo anterior en el sector Defensa el área de capacidad de TIC comprende las capacidades de direccionamiento estratégico y servicios de comunicaciones e informática que se requieren, relacionadas con las tecnologías necesarias para la gestión y transformación de la información; al uso de equipos y programas que permiten crear, modificar, almacenar, proteger, recuperar y actualizar la información y tecnología.

A partir de lo anterior se definen las 38 capacidades TIC del sector defensa como apoyo a las áreas misionales de las cuales el Grupo de Tecnologias de la información prioriza nueve así:

No.	Nombre Capacidad	Definición
TIC 2	Arquitectura Empresarial de TIC	Diseñar, implementar y mantener lineamientos y estándares tecnológicos y de sistemas de información en la Fuerza Pública que permita analizar integralmente las entidades que la conforman, con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria, apoyando la gestión TIC, investigación, atención al ciudadano y generando valor a través de las TIC

TIC 4	Servicios de TIC a Nivel Estratégico, Operativo y Táctico	Proveer, mantener e interoperar las redes y sistemas de comunicaciones e informática existentes en las Fuerzas Militares y Policía Nacional, en todos los niveles.
TIC 9	Integración de Sistemas de Comunicaciones	Soportar la integración de las comunicaciones entre tropas terrestres, navales, fluviales y aéreas de la Fuerza Pública, en operaciones conjuntas, coordinadas e interagenciales
TIC 12	Almacenamiento y Procesamiento de Información (Data center)	Proyectar, implementar y soportar los procesos administrativos y operativos, de la Fuerza Pública, para proveer los data center garantizando la conectividad de la infraestructura tecnológica y de comunicaciones, servicios en la nube (Cloud - Computing), Multicanalidad, Seguridad, Comunicaciones Unificadas y de voz, Servicios de Aplicación, bases de datos, plan de recuperación de desastres (DRP), centros de datos alternos entre otros.
TIC 20	Sistemas de Información Sectoriales	Proyectar, Implementar, Soportar y garantizar la funcionalidad de los sistemas de información del Sector y Defensa que son de uso común entre las Fuerzas (SIATH, SILOG-SAP, SIJUR, FOCIS, entre otros)
TIC 33	Soporte de Redes de Telecomunicaciones y Datos	Soportar y mantener la disponibilidad de la red de datos, backbone, fibra óptica, conmutación, redes LAN, redes WAN, red satelital y de las redes fijas y móviles de voz (HF, VHF, UHF), datos y video, Internet
TIC 34	Soporte de Infraestructura Informática (hardware y software)	Soportar, mantener, supervisar e inspeccionar de formar permanente la infraestructura de servidores, sistemas de climatización de centros de cómputo, detección y extinción de incendios, plataforma de cómputo, equipos activos, sistemas de almacenamiento, SIART, sistemas de visualización y audiovisuales, bases de datos, licenciamiento, integración y migración de sistemas de información, plataforma GIS, plataforma de analítica de video.
TIC 36	Soporte a Ciberdefensa	Planear, implementar, mantener y soportar el componente tecnológico y las plataformas de investigación y aseguramiento de la infraestructura propia para el desarrollo de las operaciones cibernéticas y ciberseguridad FFMM.
TIC 37	Soporte a Ciberseguridad PNC	Planear, implementar, mantener y soportar el componente tecnológico y las plataformas de aseguramiento, investigación, ciberprevención, ciberinteligencia, ciberterrorismo, cibercrimen y atención de incidentes de seguridad.

8.2 ACTIVIDADES ESTRATÉGICAS

El Hospital Militar Central tiene planteadas las siguientes actividades para el lapso 2018-2022 asi:

PROYECTO	TIEMPO	CAPACIDAD QUE IMPACTA
Estrategia de Continuidad de servicios de TI	2019-2022	TIC 12 Almacenamiento y Procesamiento de Información (Data center)
Mejoramiento de atención al usuario	2021-2022	TIC-34 Soporte de Infraestructura Informática (hardware y software)
Implementación de plataforma para educación virtual	2019-2022	TIC 20- Sistemas de Información Sectoriales
Mejoramiento del sistema de gestión documental	2019-2022	TIC 20- Sistemas de Información Sectoriales
Actualización servidores, migración y Licenciamiento Oracle	2019	TIC 12 Almacenamiento y Procesamiento de Información (Data center) TIC 34 Soporte de Infraestructura Informática (hardware-Software)
Licenciamiento y mantenimiento de herramientas ofimáticas, pagina web, intranet, red social.	2018-2022	TIC 34 Soporte de Infraestructura Informática (hardware-Software)
Licenciamiento y Mantenimiento herramientas de Seguridad	2018-2022	TIC-36 Soporte a Ciberdefensa
Dotación Tecnológica y Mantenimiento Centros de Cableado, redes, equipos de cómputo y comunicaciones	2018-2022	TIC 34 Soporte de Infraestructura Informática (hardware-Software)
Mantenimiento Sistemas de información institucional y de apoyo	2018-2022	TIC 20- Sistemas de Información Sectoriales

Teniente **Coronel Ariadna Ramirez Ospina**
Jefe de Unidad de Seguridad y Defensa
Unidad de Informática