DIRECCIÓN GENERAL
DE SANIDAD MILITAR
Un equipo humano al servicio de la salud

Plan Estratégico de Tecnologías de la Información y las Comunicaciones

2023-2026

CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de los cambios
1	Enero 2023	Se ajustó el documento, por actualización de guía para la formulación y seguimiento de planes institucionales MDN-COGFM-PROPLAES-DIGSA-GI.95.1-3. Presentado mediante Acta No. 0122014671502 del 21 de diciembre 2022. NOTA PROASIG – PROPLAES Este documento fue revisado por PROASIG, cumple con los requisitos establecidos en el formato establecido por el Sistema Integrado de Gestión SIG, para aprobarlo en la SVE; PROPLAES libera el documento. La información registrada en el documento es responsabilidad del proceso que lo emite.
2	Septiembre 2023	Se ajustó el documento, por actualización de guía para la formulación y seguimiento de planes institucionales MDN-COGFM-PROPLAES-DIGSA-GI.95.1-3. Se aclara que en la versión 1, No fue aprobado, fue revisado mediante Acta No. 0122014671502 del 21 de diciembre 2022. En esta versión se ajusta el documento, por actualización de la guía para la formulación y seguimiento de planes institucionales MDN-COGFM-PROPLAES-DIGSA-GI.95.1-1 vigencia 2023. Se ajusto acorde a las observaciones realizadas en la versión 1, acta No. 0122014671502 del 21 de diciembre 2022 y es aprobado por el Acta 0123010218102 del Comité Institucional de Gestión y Desempeño del 15 de septiembre del 2023 NOTA PROASIG – PROPLAES 1. Este documento fue revisado por PROASIG, PROPLAES libera el documento. 2. La información registrada en el documento es responsabilidad del proceso que lo emite. 3. Este documento fue construido de acuerdo con los parámetros de lenguaje claro emitidos por el Departamento Nacional de Planeación
3	Enero 2024	Se presento el documento al Comité institucional de gestión y desempeño el cual fue aprobado mediante Acta No. 0123013530002MDN-COGFM-JEMCO-DIGSA-GRUPL-ARDEI-29.75 del 05 de diciembre 2023. NOTA PROASIG – PROPLAES

		1. Este documento fue revisado por PROASIG, PROPLAES libera el documento. 2. La información registrada en el documento es responsabilidad del proceso que lo emite. 3. Este documento fue construido de acuerdo con los parámetros de lenguaje claro emitidos por el Departamento Nacional de Planeación

CONTROL DE APROBACIÓN

<table>
<tr><td>Aprobó:</td><td colspan="2">CR. Alexander Peña Cristancho
Subdirector Técnico y de Gestión DIGSA</td></tr>
<tr><td rowspan="3">Revisó:</td><td>TAST. Yamile López
Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones PROGTIC
Gestora de Calidad</td><td>TC. Elizabeth Bocarejo Bautista
Coordinadora Grupo Sistema Integral de Tecnologías de la Información y Comunicación DIGSA</td></tr>
<tr><td colspan="2">PD. Silvestre Granados Silva
Coordinador Grupo Gestión de la Información DIGSA</td></tr>
<tr><td>SMSM. Edna del Pilar Martínez Páez
Grupo Planeación Estratégica DIGSA
Líder Área Sistemas Integrados de Gestión PROASIG</td><td>PD. Alexandra Martínez Vargas
Coordinadora Grupo Planeación Estratégica DIGSA
Representante de la Alta Dirección</td></tr>
<tr><td>Elaboró:</td><td colspan="2">PD. Alexandra Mora Nova
Grupo Gestión de la Información DIGSA
Área Coordinación y Suministro de Información</td></tr>
</table>

TABLA DE CONTENIDO

1. PRESENTACION PETI 2023-2026

La Dirección General de Sanidad Militar, en línea con las políticas establecidas en el Marco del Plan Nacional de Desarrollo y congruente con el Plan Estratégico de Tecnologías de la Información del Ministerio de Defensa Nacional y del Ministerio de Tecnologías de la Información y las Comunicaciones, establece criterios institucionales para estandarizar todos los temas asociados a las TIC y generar una integración de los mismos, aumentar las capacidades, establecer mecanismos de uso y apropiación tendientes a optimizar los procesos de la Dirección así como establecer mecanismos de control para toma de decisiones informadas y en tiempo real.

Para el efecto se hace necesario cumplir con los criterios de la información, los cuales se basan en la disponibilidad, confiabilidad y accesibilidad, estableciendo las siguientes líneas de acción:

Primero: Garantizar la infraestructura de las redes WAN y LAN de la DIGSA, con el fin de mantener alta disponibilidad de los canales, sin que genere pérdida de información, y a su vez gestionar desde su competencia ante los Comandos de Fuerza y el Gobierno Corporativo en salud el estado operativo de los canales de las mismas en los Establecimientos de Sanidad Militar.

Las Direcciones de Sanidad y la Jefatura de Salud, a su vez gestionaran lo pertinente a su nivel dentro de cada Fuerza.

Segundo: Garantizar la disponibilidad de las TIC en la DIGSA, para mantener operativo el sistema de información y las comunicaciones.

Tercero: La DIGSA debe contar con un plan de obsolescencia de equipos de cómputo, software y servidores garantizando contar con tecnología de punta que permita la incorporación de nuevas tecnologías y factores de seguridad vitales para garantizar operatividad y a su vez gestionar desde su competencia, lo pertinente ante los Comandos de Fuerza y el Gobierno Corporativo en salud.

Las Direcciones de Sanidad y la Jefatura de Salud, a su vez gestionaran lo pertinente a su nivel dentro de cada Fuerza.

Cuarta: Implementar las fases estratégicas del gobierno de datos (planeación y diseño, habilitación y movimiento, uso y mejoras y actividades funcionales) como componentes del ciclo de vida de los datos, con el fin de respaldar la toma de decisiones.

Quinto: Fortalecer los mecanismos TIC’s de interacción con los afiliados y beneficiarios del Subsistema de salud, en el marco de la misión de garantizar el acceso a la prestación servicios de salud.

Sexto: Optimizar y administrar los centros de datos de la Dirección General de Sanidad Militar, con el fin de mejorar la capacidad de procesamiento, disponibilidad y seguridad, de la información de la institución.

Séptimo: Propender por la apropiación del conocimiento proyectando el diseño y planeación del Sistema de Seguridad de la Información, Modelo de Seguridad y Privacidad de la Información y la ISO 27001, con su implementación faseada al 2026, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información, así como difundirlo a las Direcciones de Sanidad y la Jefatura de Salud para que a su nivel se coordine y/o articule lo pertinente dentro de cada Fuerza.

2. OBJETIVO DEL DOCUMENTO

La Dirección General de Sanidad Militar se propone contar con un Plan Estratégico de Tecnologías de la Información (PETI) que responda a la situación actual de las TIC en la organización, identificando sus necesidades y oportunidades de mejora. Este plan proyecta, a través de la ejecución de actividades e iniciativas estratégicas, el fortalecimiento de las capacidades tecnológicas institucionales, en cumplimiento con la normatividad vigente.
El PETI tiene como objetivo orientar la implementación de soluciones tecnológicas en los Establecimientos de Sanidad Militar, con el fin de mejorar la eficiencia en la gestión y contribuir a la calidad en la prestación de los servicios de salud. De esta manera, se busca una integración efectiva de las TIC como herramienta habilitadora del servicio, en armonía con las políticas sectoriales y los lineamientos del sector Defensa y Salud.

3. ALCANCE DEL PETI

El Plan Estratégico de Tecnologías de la Información y Comunicaciones 2023 - 2026, incluye para su ejecución, los Grupos de trabajo de la DIGSA, con el enfoque estructurado, está alineado con los dominios definidos en el modelo de gestión, estrategia, gobierno, información, sistemas de información, infraestructura de TI, uso, apropiación y seguridad.

Los demás actores del Subsistema de Salud de las Fuerzas Militares, conformado por la Dirección de Sanidad del Ejercito Nacional (DISAN EJC) Dirección de Sanidad de la Armada Nacional (DISAN ARC), Jefatura Salud Fuerza Aeroespacial Colombiana (JEFSA), gestionarán lo pertinente a su nivel de competencia, dentro de cada Fuerza.

El presente Plan Estratégico, se convierte en la guía principal sobre la cual deben estructurar y definir la planeación y gestión tecnológica, la mejora de procesos internos y el intercambio de información de los proyectos de TI., el aprovechamiento de la información para el análisis, la toma de decisiones y el mejoramiento permanente hacia una eficaz gestión institucional.

El liderazgo de su implementación se encuentra a cargo del Grupo Sistema Integral de Información - Tecnologías de la Información y las Comunicaciones (SISAM).

4. FUNDAMENTO NORMATIVO

El Plan Estratégico de Tecnologías de la Información – PETIC 2023-2026, se ajustan a la normatividad vigente que rige al Subsistema de Salud de las Fuerzas Militares, y se encuentra documentada en el normograma, a partir del cual tienen sustento el desarrollo e implementación de la tecnología y los sistemas de información en la institución pública, de acuerdo con el ente rector que es el Ministerio de las TIC.

- Constitución Política de Colombia de 1991, Artículo 15. “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
- Ley 9 de 1979, “Código Sanitario Nacional”.
- Ley 23 de 1982, “Sobre Derechos de Autor. Congreso de la República”.
- Ley 100 de 1993, “Por la cual se crea el Sistema de Seguridad Social Integral y se dictan otras disposiciones” – Aplica solo el artículo 279.
- Ley 352 de 1997, “Por la cual se reestructura el Sistema de Salud de las Fuerzas Militares y la Policía Nacional y se dictan otras disposiciones en materia de seguridad social para las Fuerzas Militares y la Policía Nacional”.
- Ley 527 de 1999, “Por 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 962 de 2005, “Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estadoy de los particulares que ejercen funciones públicas o prestan servicios públicos”.
- Ley 1122 de 2007, “Por la cual se hacen algunas modificaciones en el Sistema General de Seguridad Social en Salud y se dictan otras disposiciones”.
- 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 dela 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 -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones”.
- Ley 1438 de 2011, “Por medio de la cual se reforma el Sistema General de Seguridad Social en Salud y se dictan otras disposiciones”.

- Ley 1581 de 2012, “Por el cual se dictan disposiciones generales para la protección de datos personales”.

- Ley 1672 de 2013, “Por la cual se establecen los lineamientos para la adopción de una política pública de gestión integral de residuos de aparatos eléctricos y electrónicos (RAEE), y se dictan otras disposiciones.”

- Ley 1712 de 2014, “Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.

- Ley 1751 de 2015, “Por medio de la cual se regula el derecho fundamental a la saludy se dictan otras disposiciones.”

- Ley 1978 de 2019, “Por la cual se moderniza el Sector de las Tecnologías de la información y las Comunicaciones – TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones”.

- Ley 2294 del 19 de mayo del 2023, “Por el cual se expide el Plan Nacional de Desarrollo 2022- 2026 "Colombia potencia mundial de la vida”.

- Decreto Ley 1795 de 2000, “Por el cual se estructura el Sistema de Salud de las Fuerzas Militares y la Policía Nacional”.

- Decreto Ley 19 de 2012, “Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública”.

- Decreto 1796 de 2000, “Por el cual se regula la evaluación de la capacidad sicofísicay de la disminución de la capacidad laboral, y aspectos sobre incapacidades, indemnizaciones, pensión por invalidez e informes administrativos por lesiones, de los miembros de la Fuerza Pública, Alumnos de las Escuelas de Formación y sus equivalentes en la Policía Nacional, personal civil al servicio del Ministerio deDefensa Nacional y de las Fuerzas Militares y personal no uniformado de la Policía Nacional vinculado con anterioridad a la vigencia de la Ley 100 de 1993”.

- Decreto 2330 de 2006, “Por el cual se modifica el Decreto 2200 de 2005 y se dictan otras disposiciones”. Ministerio de Salud y Protección Social.

- Decreto 4782 de 2008, “Por el cual se modifica la estructura del Ministerio de Defensa Nacional- Dirección General de Sanidad Militar y se dictan otras disposiciones”.

- Decreto 2482 de 2012, “Por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión”.

- Decreto 2693 de 2012, “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones”.

- Decreto 1377 de 2013, “Por el cual se reglamenta parcialmente la Ley 1581 de 2012”.

- Decreto 333 de 2014, “Por el cual se reglamenta el artículo 160 del Decreto-ley 19 de 2012”.

- Decreto 886 de 2014, “Reglamentar la información mínima que debe contener el Registro Nacional de Bases de Datos, creado por la Ley 1581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los responsables de Tratamiento”.

- Decreto 103 de 2015, “Por el cual se reglamenta parcialmente la Ley 1712 de 2014 en lo relativo a la gestión de la información pública y se dictan otras disposiciones”.

- Decreto 1066 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector Administrativo del Interior".

- Decreto 1074 de 2015, “Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo”.

- Decreto 1078 de 2015, “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

- Decreto 1080 de 2015, “Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura”.

- Decreto 1083 de 2015, “Por el cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el cual incluye el Decreto 2573 de 2014 que establece los lineamientos generales de la Estrategia de Gobierno en Línea (Hoy Gobierno Digital)”.

- Decreto 1494 de 2015, “Por el cual se corrigen yerros en la Ley 1712 de 2014”.

- 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”.

- Decreto 1412 de 2017, “Por el cual se adiciona el título 16 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para reglamentarse los numerales 23 y 25 del artículo 476 del Estatuto Tributario”.

- Decreto 1413 de 2017, “Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título 111 de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales”.

- Decreto 1414 de 2017, “Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones y se dictan otras disposiciones”.

- Decreto 2194 de 2017, “Decreto modificatorio del artículo 2.2.2.4.1 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto número 1078 de 2015”.
- Decreto 611 de 2018, “Por el cual se derogan unas comisiones intersectoriales”.

- Decreto 612 de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”.

- Decreto 90 de 2018, “Serán objeto de inscripción en el Registro Nacional de Bases de Datos, las bases de datos que contengan datos personales cuyo Tratamiento automatizado o manual sea de sociedades y/o entidades sin ánimo de lucro y personas jurídicas de naturaleza pública”.

- Decreto 1008 de 2018, “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015”.

- Decreto 2106 de 2019, "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública”. Aplica el Capítulo II Transformación Digital Para Una Gestión Pública Efectiva.

- Decreto 620 de 2020, “Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales”.

- Decreto 441 del 28 de marzo 2022, “Por medio del cual sustituye el Capítulo 4 del Título 3 de la parte 5 del libro 2 del decreto 780 de 2016 relativo a los acuerdos de volúmenes entre las unidades responsables de pago, los prestadores de servicio de salud y los proveedores de tecnologías en salud”.

- Decreto 1263 del 22 de Julio 2022, “Por el cual se adiciona el Titulo 22 a la parte 2 del libro 2 del decreto 1078 del 2015, Decreto Único Reglamentario del Sector de la Tecnología de la información y las comunicaciones, con el fin de definir lineamientosy estándares aplicables a la Transformación Digital Pública”.

- Resolución 3374 de 2000, “Por la cual se reglamentan los datos básicos que deben reportar los prestadores de servicios de salud y las entidades administradoras de planes de beneficios sobre los servicios de salud prestados”.

- Resolución 891 de 2009, “Por la cual se crea el Comité de Integración de Tecnologías de Información y Comunicaciones – CITI – del Sector Defensa, para fijar las políticas de estandarización en materia de tecnología, comunicaciones y servicios en el Ministerio de Defensa Nacional”.

- Resolución 8614 de 2012, “Por la cual se adopta el Programa de Gestión Documental

PGD “Hacia un Sistema de Gestión de Documento Electrónico de Archivo” – SGDEA, para el Sector Defensa”.

- Resolución 1537 de 2015, “Por la cual se determinan las especificaciones técnicas para la consulta en línea de forma masiva, de la fe de vida o supervivencia de las personas y mecanismo de transferencia de los archivos”.
- Resolución 3202 de 2016, “Por la cual se adopta el Manual Metodológico para la elaboración e implementación de las Rutas Integrales de Atención en Salud — RIAS, se adopta un grupo de Rutas Integrales de Atención en Salud desarrolladas por el Ministerio de Salud y Protección Social dentro de la Política de Atención Integral en Salud —PAIS y se dictan otras disposiciones”.

- Resolución 2710 de 2017, “Por la cual se establecen lineamientos para la adopción del protocolo IPv6”.

- Resolución 774 de 2018, “Por la cual se adoptan los límites de exposición de las personas a los campos electromagnéticos, se reglamentan las condiciones que deben reunir las estaciones radioeléctricas para cumplirlos y se dictan disposiciones relacionadas con el despliegue de antenas de radiocomunicaciones”.

- Resolución MDN-5563 de 2018, “Por la cual se formula el PETI del Sector Defensa y Seguridad 2018-2022' y se emiten otros lineamientos relacionados con las TIC’s ylas Comunicaciones en el Sector Defensa”.

- Resolución 0322 de 2020, “Por la cual se crean y organizan grupos internos de trabajo en el Ministerio de Defensa Nacional – Comando General de las Fuerzas Militares – Dirección General de Sanidad Militar y se les asignan funciones”.

- Resolución 923 de 2020, “Por la cual se adiciona la Resolución 0322 del 11 de marzo de 2020 y se modifica la Resolución 0598 del 8 de mayo de 2020”.

- Resolución 598 de 2020, “Por la cual se adiciona la Resolución 0322 del 11 de marzo de 2020”.

- Resolución 311 de 2021, “Por la cual se modifica parcialmente la Resolución 0322 del 11 de marzo de 2020”.

- Resolución 1700 de 2021, “Por la cual se modifican las Resoluciones 0322 del 11 de marzo de 2020 y 0598 del 8 de mayo de 2020”.

- Resolución 0866 de 2021, “Por la cual se reglamenta el conjunto de elementos de datos clínicos relevantes para la interoperabilidad de la historia clínica en el país y se dictan otras disposiciones”.

- Resolución 7870 de 2022, “Por la cual se emite y adopta la Política General de Seguridad y Privacidad de la información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades

adscritas y vinculadas al sector Defensa, y se dictan otras disposiciones".

- Acuerdo 072 de 2019, "Por el cual se dictan políticas generales y lineamientos para la organización del Sistema de Salud de Fuerzas Militares y de la Policía Nacional".

- Circular 12 de 2007, "Verificación, recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derechos de autor sobre programas de computador".
- Circular 17 de 2011, "Modifica Circular 12 del 02/02/2007 sobre recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia dederechos de autor sobre programas de computador (software)".

- Circular 406948/MDN de 2016, "Se emite lineamiento para uso del Formato generado por el sistema de información SALUD.SIS".

- Circular 8187 de 2019, "Lineamientos para la Implementación de los Procesos de Soporte y Mantenimiento del Sistema Integral de Información SALUD.SIS".

- Directiva Presidencial 09 de 2010, "Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones pública".

- Directiva Presidencial 04 de 2012, "Eficiencia Administrativa y Lineamientos de la Política Cero Papel en la Administración Pública".

- Directiva 2018-272/MDN, "La utilización de servicios en la nube, se debe realizar bajo los siguientes parámetros: servicios de CLOUD debe ser clara las obligaciones del contratista en cuanto a la responsabilidad respecto a la conservación de los contenidos (información), borrado de datos, propiedad intelectual y niveles de servicio (ANS)".

- Directiva Permanente 02 de 2002, "Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software)".

- Directiva Permanente 913 de 2013, "Guías y procedimientos en tecnología de información y comunicaciones para el Sector Defensa".

- Directiva Permanente 2014-18, "Políticas de Seguridad de la información para el Sector Defensa".

- Directiva Permanente 154 de 2014, "Políticas de seguridad de la información para las Fuerzas Militares".

- Directiva Permanente 0118000010005 /MDN de 2018, "Dar lineamientos y directrices para la planificación, administración y articulación de las TIC's a nivel FFMM con la Estandarización, integración de las capacidades en apoyo al desarrollo de operaciones conjuntas".

- Directiva Permanente 3 de 2019, "Política de privacidad y protección de datos; define

los lineamientos la política de tratamiento de datos personales en el Ministerio de Defensa".

- Directiva Permanente 2014-18 de 2021, "Implementación de un sistema de seguridad de la información y estandarización de las Políticas de Seguridad de la información para el sector Defensa".

- CONPES 3854 de 2016, "Política Nacional de Seguridad Digital".

- CONPES 3920 de 2018, "Política Nacional de Explotación de Datos (BIG DATA)".

- CONPES 3975 de 2019, "Política Nacional para la Transformación Digital e Inteligencia Artificial".

- CONPES 3995 de 2020, "Política Nacional de Confianza y Seguridad Digital".

- Manual 1 de 2012, "Manual de Políticas de seguridad de la información Dirección General de Sanidad Militar".

- Guía No. 5 Versión No. 1 de 2016, "Guía para la Gestión y Clasificación de Activos de Información del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC)".

- Guía Versión No. 4 de 2018, "Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital".

- Guía No. 6 Versión 1.1. de 2019, "Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI".

- Norma Técnica ISO/IEC 20000 de 2005, "Estándar internacional para la gestión de servicios de TI (Tecnologías de la Información)".

- Norma Técnica ISO 12207:2008 de 2006, "El estándar para los procesos de ciclo de vida del software de la organización".

- Norma Técnica ISO 27001:2013 de 2013, "Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos".

- Norma Técnica ISO 27000:2016 de 2016, "Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información (SGSI)".

- Norma Técnica ISO 31000 de 2017, "Gestión de Riesgos Empresariales".

5. DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

Amenaza: Causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

Análisis de riesgos: Proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.

Confidencialidad: Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Control: Comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Gestión del riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Incidente de seguridad de la información: Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad o disponibilidad de la información.

Información: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

Integridad: Cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Política de seguridad de información: Es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Privacidad: La capacidad que una organización o individuo tiene para determinar qué datos pueden ser compartidos.

Procedimiento: Forma específica de llevar a cabo una actividad o un proceso.

Proceso: Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Propietario de activo de información: Identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

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.
Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o de los procesos de la DIGSA. Se expresa en términos de probabilidad y consecuencias.

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Vulnerabilidad: Debilidad de un activo o control que pueda ser explotado por una o más amenazas.

6. ACRÓNIMOS

DIGSA - Dirección General de Sanidad Militar

GRUPL - Grupo Planeación Estratégica.

LAN - Red de área Local

PROGTIC - Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones.

PROGI - Proceso Gestión de la Información.

SISAM - Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones.

PROGAFI - Proceso Gestión de la Afiliación.

PROAUPS - Proceso Atención al Usuario y Participación Social.

PROGACAS - Proceso Garantía de la Calidad en Salud.

PROPRES - Proceso Prestación y Operación de Servicios de Salud.

PROSOPE - Proceso Salud Operacional.

PROAS - Proceso Aseguramiento en Salud.

PROGRERI - Proceso Gestión del Riesgo en Salud.

PROAPA - Proceso Apoyo Administrativo.

PROEFIN - Proceso Ejecución Financiera.

PROTH - Proceso Talento Humano.

PROCOM - Proceso Gestión Contratación.

PROGI - Proceso Gestión de la Información.

PROPOSE - Proceso Salud Operacional.

PROALEG - Proceso Asuntos Legales.

PROSYEIN - Proceso Seguimiento y Evaluación.

SSMP - El Sistema de Salud de las Fuerzas Militares y de la Policía Nacional

TIC - Tecnología de la información y las Comunicaciones

WAN - Red de área amplia

7. MARCO CONCEPTUAL

El Plan Estratégico de Tecnologías de la Información (PETI) de la Dirección General de Sanidad Militar (DIGSA) es el resultado del trabajo estratégico liderado por la Subdirección Técnica y de Gestión (SUBTG), orientado a planificar de manera efectiva las acciones relacionadas con la adquisición, desarrollo, soporte, mantenimiento, uso y apropiación de las tecnologías de la información.

Este plan busca garantizar que los objetivos de TI estén plenamente alineados con las metas institucionales, fortaleciendo la capacidad operativa y estratégica de la Entidad.

El PETI 2023–2026 es un instrumento flexible y dinámico, diseñado para adaptarse a los cambios del entorno, normativas y lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Su formulación se sustenta en cuatro motivadores estratégicos clave: Estrategia Nacional, Estrategia Sectorial, Estrategia Institucional y Lineamientos y Políticas, asegurando así su coherencia con las prioridades del sector Defensa y del Gobierno Nacional.

7.1 Motivadores Estratégicos

Esta sección del documento hace referencia a los motivadores de negocio identificados estratégicamente para la DIGSA que direccionarán la estrategia de TI para la entidad y Políticas que dan línea en la orientación y alineación de la Estrategia de Tecnologías de la Información - (PETI).

Ilustración 1. Alineación Estratégica DIGSA

7.2 Estrategia Nacional

Plan Nacional de Desarrollo 2022-2026; Área Misional: Gestión, apoyo y Desarrollo Proyectivo; OBJ. 11 bienestar y seguridad jurídica de los miembros de la Fuerza Pública.

Política Defensa y Seguridad; OBJ. 7 garantizar protección, profesionalización y bienestar de los miembros de las Fuerzas Militares, la Policía Nacional y sus familias.

7.3 Estrategia Sectorial

Plan Estratégico Sectorial 2019-2022; OBJ. 11 garantizar el bienestar, la salud y la seguridad jurídica de los miembros de las Fuerzas Militares y Policía.

META 2: Mejorar el Sistema de Salud de las Fuerzas Militares y Policía Nacional.

7.4 Estrategia Institucional

Plan de Desarrollo Institucional 2019-2022; OBJ. 3 fortalecer el desarrollo, implementación e integración del Sistema de Información en los procesos de aseguramiento y la prestación de los servicios de salud.

7.5 Lineamientos y políticas

El personal trabajará con los siguientes lineamientos y/o principios:

- Gestionar y administrar las TIC bajo los principios de la DIGSA: Además de los principios generales de ética, equidad, universalidad y eficiencia, serán orientadores de la actividad de los órganos que constituyen el SSMP, enmarcados en la Ley 352 de 1997 los siguientes:

    a. Racionalidad. El SSMP utilizará los recursos de manera racional a fin de que los servicios sean eficaces, eficientes y equitativos.

    b. Obligatoriedad. Es obligatoria la afiliación de todas las personas enunciadas en el artículo 19 de la presente ley sin perjuicio de lo dispuesto en el literal a), numeral 7 del mismo artículo.

    c. Equidad. El SSMP garantizará servicios de salud de igual calidad a todos sus afiliados y beneficiarios, independientemente de su ubicación geográfica, grado o condición de uniformado o no uniformado, activo, retirado o pensionado. Para evitar toda discriminación, el SSMP informará periódicamente a los organismos de control, las actividades realizadas, detallando la ejecución por grados y condiciones de los anteriores usuarios.

    d. Protección integral. EL SSMP brindará atención en salud integral a sus afiliados y beneficiarios en sus fases de educación, información y fomento de la salud, así como en los aspectos de prevención, diagnóstico, tratamiento, rehabilitación, en los términos y condiciones que se establezcan en el plan de Servicios de Sanidad Militar y Policial, y atenderá todas las actividades y suministros que en materia de salud operacional requieran las Fuerzas Militares y la Policía Nacional para el cumplimiento de su misión. En el SSMP no existirán restricciones a los servicios prestados a los afiliados y beneficiarios por concepto de preexistencias.

e. Autonomía. El SSMP es autónomo y se regirá exclusivamente de conformidad con lo establecido en la presente ley.

f. Descentralización y desconcentración. El SSMP se administrará en forma descentralizada y desconcentrada en las Fuerzas Militares y en la Policía Nacional con sujeción a las políticas, reglas, directrices y orientaciones trazadas por el Consejo Superior de Salud de las Fuerzas Militares y de la Policía Nacional.

g. Unidad. El SSMP tendrá unidad de gestión, de tal forma que, aunque la prestación de servicios se realice en forma desconcentrada o contratada, siempre exista unidad de dirección y políticas, así como la debida coordinación entre los subsistemas y entre las entidades y unidades de cada uno de ellos.

h. Integración funcional. Las entidades que presten servicios de salud concurrirán armónicamente a la prestación de estos mediante la integración en sus funciones, acciones y recursos, de acuerdo con la regulación que para el efecto adopte el Consejo Superior de Salud de las Fuerzas Militares y de la Policía Nacional.

i. Independencia de los recursos. Los recursos que reciban las Fuerzas Militares y la Policía Nacional para la salud deberán manejarse en fondos cuenta separados e independientes del resto de su presupuesto y sólo podrán destinarse a la ejecución de dichas funciones.

j. Atención equitativa y preferencial. Todos los niveles del SSMP deberán atender equitativa y prioritariamente a los afiliados y beneficiarios de este. Por consiguiente, solamente podrán ofrecer servicios a terceros o a entidades promotoras de salud, una vez hayan sido satisfechas debidamente las necesidades de tales usuarios y previa autorización del Consejo Superior de Salud de las Fuerzas Militares y de la Policía Nacional.

- Promover y desarrollar las Tecnologías de la Información y las Comunicaciones en las diferentes dependencias de la DIGSA con el propósito de infundir el uso y apropiación de estas.

- Mantener las necesidades de TIC que usa la DIGSA con flexibilidad y resiliencia.

- La inversión debe corresponder al desarrollo y/o sostenimiento de las actividades e infraestructura estratégica y al cumplimento de los objetivos definidos por la DIGSA.

- Las soluciones tecnológicas propuestas deben responder a necesidades institucionales y transversales de integración del Sector más que a requerimientos institucionales.

- Se debe desarrollar las TIC con el ánimo de acortar las brechas identificadas cumpliendo con el modelo de gestión desarrollado.

- Enfocar los proyectos de arquitectura a las directrices establecidas por el área de tecnología cabeza del Sector.

8. MODELO OPERATIVO

Para la operación de la Dirección General de Sanidad Militar se cuenta con la descripción de alto nivel del mapa de procesos, la cual representa el comportamiento que está dando orientación al cómo gestiona las actividades para dar cubrimiento a la misionalidad.

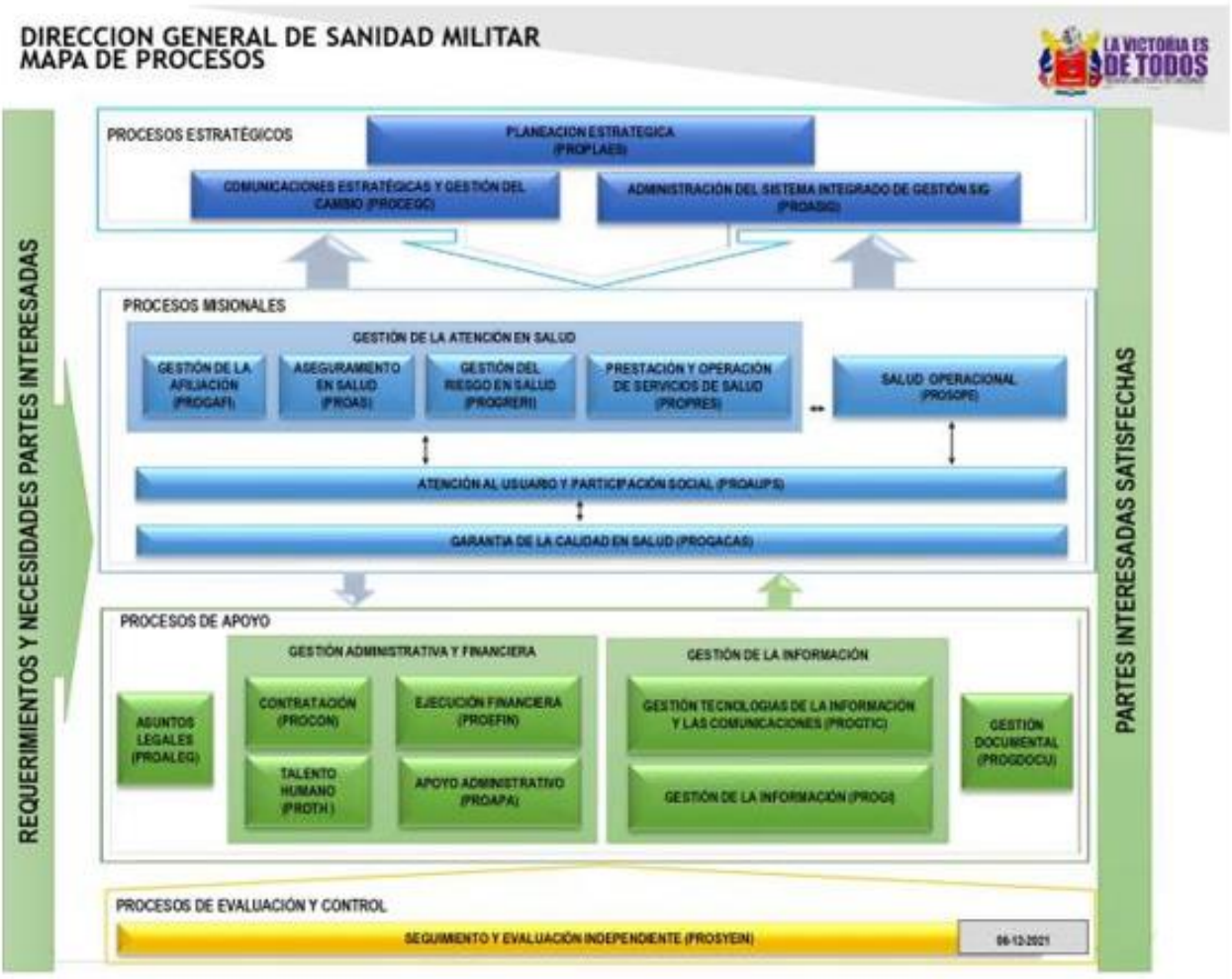


Ilustración 2. Mapa de procesos DIGSA

8.1. Descripción de procesos

8.1.1. Procesos estratégicos

Tabla 1. Procesos estratégicos

Abreviación	Nombre	Objeto
PROPLAES	Planeación Estratégica	Direccionar a la entidad a través de la formulación de estrategias, planes, programas, proyectos y evaluación de la gestión., para asegurar el cumplimiento de la misión institucional.

PROASIG	Administración del Sistema integrado de Gestión SIG	Diseñar, documentar, implementar, mantener y hacer seguimiento al sistema de gestión integrado, mediante las correspondientes acciones formuladas, teniendo como premisa el mejoramiento continuo.
PROCECC	Comunicación estratégica y Gestión del Cambio	Generar estrategias que permitan la difusión de información, así como el apoyo a la transformación y el cambio de la imagen institucional, teniendo en cuenta la misión del subsistema de Salud de las Fuerzas Militares y la gestión de la organización, con el fin de mantener informados los grupos de interés y confianza a través de información verídica, transparente, actualizada y con lenguaje claro.

Fuente: Elaboración propia GRUGI.

Estos procesos cuentan con las siguientes aplicaciones:

- Portal Web y Portal **Salud.SIS**: Canales de comunicación oficiales de la Entidad, de cara al ciudadano y al usuario, ofrecen servicios en línea. Son un instrumento de Gobierno en línea.

- Suite Visión Empresarial: Registra la información relacionada con los planes estratégicos y funcionales de la Entidad.

- WEB -PQR: Plataforma a través de la cual los usuarios del Subsistema de Salud de las Fuerzas Militares pueden ejercer su derecho a presentar de manera respetuosa quejas, reclamos, sugerencias y felicitaciones, respecto a cualquier trámite o servicio que sea competencia de la DIGSA y sobre el cual se presente algún grado de inconformidad, por falta de oportunidad de la información, desarrollo de la actuación, así como de la deficiencia o baja calidad de esta.

8.1.2. Procesos misionales

Tabla 2. Procesos Misionales

Abreviación	Nombre	Objeto
PROGAFI	Afiliaciones	Garantizar la accesibilidad al subsistema de salud de las fuerzas militares a los usuarios afiliados y sus beneficiarios mediante el adecuado tratamiento de la información contenida en Bases de Datos, que permita a las diferentes áreas de la Dirección General de Sanidad Militar gestionar el riesgo en salud y la adecuada prestación de servicios médicos en el subsistema de salud de las Fuerzas Militares a través de la Dirección de Sanidad, Jefatura de Salud y ESM a todo nivel.
PROAUPS	Atención al usuario y participación social	Implementar el sistema de Atención al Usuario y participación social al interior del Subsistema de salud de las Fuerzas Militares a través de la gestión de las líneas de acción inherentes al mismo con mínimo el 85% de los PQRSR resueltos y el 80% en la percepción de satisfacción del usuario.
PROGACAS	Garantía de la Calidad en Salud	Realizar el seguimiento a la implementación y mantenimiento del Sistema de Calidad en Salud en las dependencias y ESM del SSFM para evaluar, monitorear y mejorar la calidad de la presentación de los servicios de salud.

Abreviación	Nombre	Objeto
PROPRES	Prestación y operación de servicios en salud	Ajustar, socializar y realizar seguimiento a los lineamientos de la normatividad vigente aplicable para la prestación de los servicios de salud a los usuarios del SSFM, a través de las Direcciones de Sanidad y Jefatura de Salud de la Fuerza Aeroespacial en los Establecimientos de Sanidad Militar para la mejora en la calidad de la prestación del servicio.
PROSOPE	Salud Operacional	El objeto de la salud operacional es mantener y recuperar la aptitud psicofísica que debe tener en todo el tiempo el personal comprometido en operaciones propias de las Fuerzas Militares, en cumplimiento de la misión constitucional, a través de la Sanidad en campaña, Medicina Naval y del Buceo y Medicina Aeroespacial, de conformidad con los programas particulares de cada fuerza
PROAS	Aseguramiento en Salud.	Validar los lineamientos y políticas vigentes, así como el seguimiento a la implementación de estas desde el aseguramiento en la prestación, atención a los servicios de salud y la suficiencia de recursos para cada usuario del subsistema de salud de las fuerzas militares
PROGRERI	Gestión del Riesgo en Salud.	Garantizar a través de las políticas y seguimiento a las mismas una atención referente, conceptual y metodológica que satisfaga los requisitos de los grupos de interés de los usuarios del Subsistema de Salud de las Fuerzas Militares.

Fuente: Elaboración propia GRUGI

- Vertical de Salud – SALUD.SIS: Sistema de información asistencial desarrollado e implementado dentro del Proyecto SALUD.SIS en el Subsistema de Salud de las Fuerzas Militares, como Vertical de Salud.

8.1.3. Procesos de apoyo

Tabla 3. Procesos de apoyo

Abreviación	Nombre	Objeto
PROAPA	Apoyo Administrativo	Administración de bienes, servicios generales y el mantenimiento de infraestructura física para la ejecución y desarrollo de los procesos de la Entidad.
PROEFIN	Gestión Financiera	Ejecutar las políticas establecidas para la administración del fondo cuenta del subsistema de salud de las Fuerzas Militares que contribuyen al cumplimiento de la misión institucional.
PROTH	Talento Humano	Formular las directrices y políticas que permiten el desarrollo, administración y el control del personal a través de condiciones de bienestar y salud en el ciclo de vida de los servidores públicos de la DIGSA, contribuyendo al aseguramiento y prestación de los servicios de SSFM.
PROCON	Contratación	Estructurar, adelantar, orientar y acompañar la gestión precontractual, de conformidad con las disposiciones legales vigentes, para el logro de la contratación oportuna de los procesos institucionales de la DIGSA.
PROGI	Grupo Gestión de la Información	Identificar en el flujo de la información las entradas y los productos, la aplicación de los mecanismos de captura y de reportes y el análisis y seguimiento a la calidad de la información en todos los procesos y procedimientos de la DIGSA.
PROCTIC	Gestión de las tecnologías de la información y las comunicaciones	Mantener operativa la Plataforma tecnológica acorde a las necesidades de la Dirección General de Sanidad Militar, mediante la administración, desarrollo, implementación, seguridad y soporte de las tecnologías de la información y las comunicaciones.
PROALEG	Grupo de Apoyo legal	Asesorar, conceptuar y apoyar, oportunamente los asuntos legales de la entidad y en materia jurídica a todas las dependencias de la DIGSA y dependencias del SSFM cuando sea requerido

Fuente: Elaboración propia GRUGI

- OnBase: Está disponible para la publicación de imágenes, reconocimiento óptico OCR de caracteres para digitalización, administración de flujos de trabajo en procesos documentales en interfaz cliente/servidor y web además herramientas para exportación de imágenes en medios portables de almacenamiento (CD/DVD) e integración documental con otras aplicaciones.

- Kactus: Sistema de Información de administración de Talento Humano y Nómina.

- Dinámica Gerencial: Sistema de información asistencial y administrativo desarrollado e implementado por un tercero como Vertical de Salud y ERP administrado por el Hospital Militar Central y Hospital Naval de Cartagena, de manera independiente.

- SECOP: Plataforma tecnológica para la gestión de la contratación estatal.

- SIIF Nación: Sistema de información para la gestión del presupuesto general de la Nación.

- ERP-SAP: Sistema de información logístico del Sector Defensa administrado por SILOG

8.1.4. Proceso de evaluación y control

Tabla 4. Proceso de evaluación y control

Abreviación	Nombre	Objeto
PROSYEIN	Grupo de Seguimiento y evaluación	Realizar seguimiento y evaluación al cumplimiento de los procesos, los planes programas y proyectos del SSFM y evaluar la efectividad del sistema de control interno de manera independiente a través de auditorías que permitan generar alertas tempranas que contribuyan al mejoramiento continuo en la gestión institucional, de acuerdo con el Plan Anual de Auditorias y los seguimientos para cada vigencia.

Fuente: Elaboración propia GRUGI

9. SITUACIÓN

9.1. Estrategia de TI

Está definida por principios, acciones y objetivos concretos que demuestran la forma como la Entidad proyecta hacer uso de las Tecnologías de la Información y Comunicaciones, fortaleciendo el direccionamiento estratégico para el logro eficiente de la entidad en la toma de decisiones para el cumplimiento de su misión.

La Estrategia de TI utilizada para desarrollar las políticas y lineamientos de las tecnologías de la información del Subsistema de Salud está enmarcada en la Directiva No. 20036 del 01 de noviembre de 2018 "Impartir las instrucciones para la continuidad del desarrollo y culminación de la implementación del Sistema Integral de Información para el Subsistema de Salud de las Fuerzas Militares.", y el Acuerdo 072 del 02 de agosto de 2019 "Por el cual se dictan políticas generales y lineamientos para la organización del Sistema Integral de Información en Salud de las Fuerzas Militares y Policía Nacional-SISMIPOL.", y fueron tenidos en cuenta en el Plan de Desarrollo 2019-2022 del Subsistema de Salud de las Fuerzas Militares en su objetivo 3 "Fortalecer el desarrollo, implementación e integración del sistema de información en los procesos de aseguramiento y la prestación de los servicios de salud.".

En el PETI 2018-2022, no se incluyeron indicadores relacionados con el monitoreo y seguimiento de la estrategia TI, por lo tanto, no se cuenta con un tablero de mando que haya permitido hacer seguimiento a los avances y resultados en el desarrollo de la Estrategia TI.

No se definieron los lineamientos, políticas y estrategias de TI sectorial por lo cual, no existe un plan estratégico de Tecnologías de la información sectorial.

9.1.1. Lienzo Estratégico Modelo de TI

Haciendo uso del modelo Lienzo Estratégico de TI, los interesados pueden ver de manera global los aspectos importantes de la gestión de Tecnologías que realiza en DIGSA.

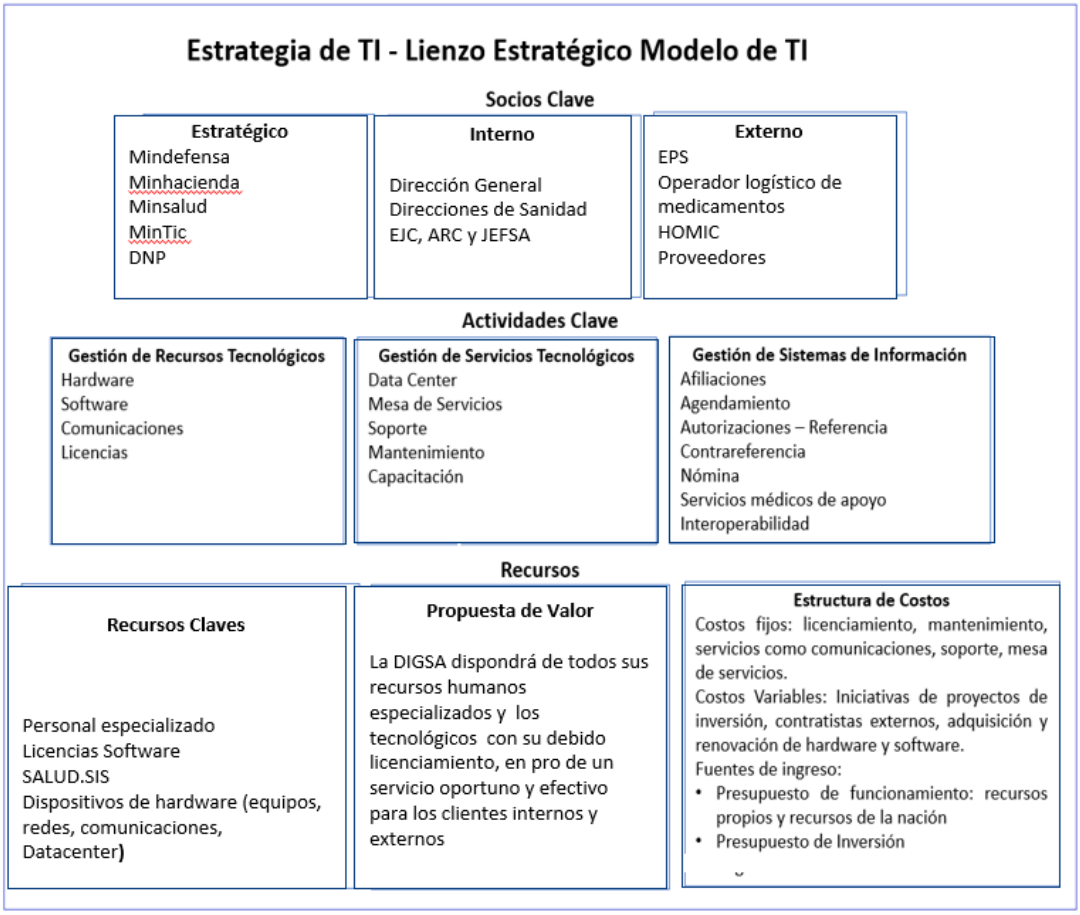


Ilustración 3. Herramienta Lienzo Estratégico

9.1.2. Misión de TI

Atender y satisfacer las necesidades de Tecnologías en Salud del Subsistema de Salud de las Fuerzas Militares, manteniendo el sistema de información, la infraestructura de tecnológica y la gestión biomédica para la coordinación entre ellas. A los usuarios, proporcionarle un servicio eficiente y expedito mediante el uso de las mejores tecnologías de la información que contribuya a una excelente atención a los usuarios, obteniendo siempre una mejora continua en el uso de las TIC´s.

9.1.3. Visión de TI

Llegar a ser un centro de información que cuente con la tecnología de vanguardia en el campo de las comunicaciones, cómputo, manejo de información, monitoreo, así como en la utilización de un sistema de información de alto nivel para proporcionar servicios de calidad a los establecimientos y direcciones de sanidad militar.

9.1.4. Matriz DOFA - Análisis Interno y Externo

La situación actual que se presenta a continuación describe como se encuentra la entidad al interior y exterior por medio de un análisis DOFA, igualmente, en la implementación del marco de arquitectura especialmente en el modelo de gestión TI, para lo cual, se evaluó la aplicabilidad de los lineamientos de cada uno de los dominios.

ENTORNO INTERNO	
FORTALEZAS	**DEBILIDADES**
F1. Se brinda soporte técnico profesional a nivel nacional para los diferentes aplicativos que se manejan. F2. Se ha apoyado por parte de la DGSM, en un 40% en redes y equipos de cómputo a los ESM. F3. Personal capacitado para dar soporte en los diferentes sistemas informáticos. F4. Normatividad vigente emitida por MINSALUD y MINTIC que nos permite alinearnos a lo establecido por la ley. F5. Se cuenta con la Vertical de Salud, desarrollada en un 60%. F6. Se cuenta con los estudios necesarios que determinan la culminación e integración de los datos del sistema de información SALUD.SIS F7. El sistema cuenta con un componente de Seguridad de la Información, a través del Comando Conjunto Cibernético del CGFM que permite proteger los datos de ataques y mantener estándares de seguridad. F8. Escalabilidad del Sistema. El sistema está diseñado para soportar los controles de cambio y aumento en el dimensionamiento del sistema, debido a que el modelo de datos puede requerir futuras modificaciones. Es conveniente tener un repositorio lo suficientemente flexible, son mejores prácticas que no pueden dejarse de aplicar. F9. SALUD.SIS, está configurado, según las necesidades de los usuarios del SSFM y por ende se encuentra identificado el portafolio de servicios de cada ESM.	D1. Falta de conocimiento en la utilización de los módulos de SALUD.SIS. D2. Recurrentes fallas en los equipos de cómputo. D3. Se presentan fallas en servidores principales de las fuerzas dificultando el trabajo en los aplicativos de red. 114 comité de Revisión Estratégica e Innovación / Salud. D4. Personal con alta rotación. D5. Sistema de información no unificado. D6. Falta de infraestructura en los ESM (Redes y Equipos). D7. Limitación de la herramienta SALUD.SIS por parametrización. D8. Falta de personal en Informática de las DISAN y DSGM para asumir la administración de SALUD. SIS. D9. Baja disponibilidad en los canales de comunicación de la red integrada de comunicaciones – RIC. D10. No se cuenta con los recursos de inversión necesarios para la culminación del sistema, generando incertidumbre de financiamiento. D11. No se ha definido la Interoperabilidad entre la Vertical de Salud y la ERP. D12. No se pueden conectar todos los ESM del SSFM, para poder tener el control total de la información de manera integral y completa que nos dé la oportunidad de tomar decisiones únicas para todo el SSFM D13. Contar con proveedores exclusivos para el Desarrollo e Implementación de SALUD.SIS, lo que implica que podemos incurrir en sobrecostos. D14. Se necesita un ERP compatible con la Vertical de Salud para integrar y automatizar los procesos. D15. Falta interconectar los equipos Biomédicos con SALUD.SIS.

	D16. Que no se asegure la contratación continua de un Datacenter para el almacenamiento de la información. D17. No se cuenta con la financiación de los costos fijos de funcionamiento de SALUD.SIS. D18. No se cuenta con el Módulo de Facturación en el proyecto de SALUD.SIS
ENTORNO EXTERNO	
OPORTUNIDADES	**AMENAZAS**
O1. Capacitación al personal que utiliza los diferentes aplicativos en el SSFM (SALUD.SIS) O2. Existencia de proveedores de hardware y software. O3. SALUD.SIS es el segundo proyecto estratégico en Salud, del Ministerio de Defensa Nacional. O4. Integrar en un Sistema la solución Vertical de Salud y la Solución ERP dentro del proyecto SALUD. SIS O5. Reducir Costos. O6. Contar con Información veraz y a tiempo, para una eficiente toma de decisiones. O7. Poder visualizar la operación total del SSFM O8. Incremento de la Productividad	A1. Las EPS privadas cuentan con tecnología de punta para realizar sus procesos. A2. Un fracaso en el proyecto del Sistema de Información en Salud conllevaría a la pérdida de credibilidad del SSFM. A3. Las EPS privadas pueden absorber el SSFM. A4. Que el CGFM no siga apoyando al SSFM en los procesos de Seguridad de la Información que hasta la fecha viene realizando de manera eficiente. A5. Existencia de equipos de cómputo con tecnología avanzada para la agilidad en los diferentes procesos.

Análisis DOFA

	OPORTUNIDADES	**AMENAZAS**
ANÁLISIS DOFA	O1. Capacitación al personal que utiliza los diferentes aplicativos en el SSFM (SALUD.SIS) O2. Existencia de proveedores de hardware y software. O3. SALUD.SIS es el segundo proyecto estratégico en Salud, del Ministerio de Defensa Nacional.	A1. Las EPS privadas cuentan con tecnología de punta para realizar sus procesos. A2. Un fracaso en el proyecto del Sistema de Información en Salud conllevaría a la pérdida de credibilidad del SSFM. A3. Las EPS privadas pueden absorber el SSFM.

	O4. Integrar en un Sistema la solución Vertical de Salud y la Solución ERP dentro del proyecto SALUD. SIS O5. Reducir Costos. O6. Contar con Información veraz y a tiempo, para una eficiente toma de decisiones. O7. Poder visualizar la operación total del SSFM O8. Incremento de la Productividad	A4. Que el CGFM no siga apoyando al SSFM en los procesos de Seguridad de la Información que hasta la fecha viene realizando de manera eficiente. A5. Existencia de equipos de cómputo con tecnología avanzada para la agilidad en los diferentes procesos.
FORTALEZAS	**ESTRATEGIAS FO**	**ESTRATEGIAS FA**
F1. Se brinda soporte técnico profesional a nivel nacional para los diferentes aplicativos que se manejan. F2. Se ha apoyado por parte de la DGSM, en un 40% en redes y equipos de cómputo a los ESM. F3. Personal capacitado para dar soporte en los diferentes sistemas informáticos. F4. Normatividad vigente emitida por MINSALUD y MINTIC que nos permite alinearnos a lo establecido por la ley. F5. Se cuenta con la Vertical de Salud, desarrollada en un 60%. F6. Se cuenta con los estudios necesarios que determinan la culminación e integración de los datos del sistema de información SALUD.SIS F7. El sistema cuenta con un componente de Seguridad de la Información, a través del Comando Conjunto Cibernético del CGFM que permite proteger los datos de ataques y mantener estándares de seguridad. F8. Escalabilidad del Sistema. El sistema está diseñado para soportar los controles de cambio y aumento en el dimensionamiento del sistema, debido a que el modelo de datos puede requerir futuras modificaciones. Es	F1-F3-O1: Fortalecer el plan de capacitación anual con los temas relacionados y actualizados con el área de Tecnologías de la Información y las Comunicaciones. F2-F7-F8-O2-O6-O8: Apoyo de la Alta Dirección en la consecución de recursos. F5-F6-F9-O3-O4-O7: Fortalecer los sistemas de información y actualizar periódicamente la arquitectura TI.	F1-F2-F3-A5: Velar por el aumento del presupuesto para la oficina TI, teniendo en cuenta los proyectos que habilitan la transformación digital. F5-F6-A2: Realizar un tablero de mandos e indicadores general para el seguimiento a los proyectos de TI. F7-A4: Adquirir el componente de Seguridad de la Información para el sistema. F8-F9-A1-A3: Implementar proyectos con tecnologías emergentes que permitan estar a la vanguardia del mercado.

conveniente tener un repositorio lo suficientemente flexible, son mejores prácticas que no pueden dejarse de aplicar. F9. SALUD.SIS, está configurado, según las necesidades de los usuarios del SSFM y por ende se encuentra identificado el portafolio de servicios de cada ESM.		
DEBILIDADES	**ESTRATEGIA DO**	**ESTRATEGIA DA**
D1. Falta de conocimiento en la utilización de los módulos de SALUD.SIS. D2. Recurrentes fallas en los equipos de cómputo. D3. Se presentan fallas en servidores principales de las fuerzas dificultando el trabajo en los aplicativos de red. 114 comité de Revisión Estratégica e Innovación / Salud. D4. Personal con alta rotación. D5. Sistema de información no unificado. D6. Falta de infraestructura en los ESM (Redes y Equipos). D7. Limitación de la herramienta SALUD.SIS por parametrización. D8. Falta de personal en Informática de las DISAN y DSGM para asumir la administración de SALUD. SIS. D9. Baja disponibilidad en los canales de comunicación de la red integrada de comunicaciones – RIC. D10. No se cuenta con los recursos de inversión necesarios para la culminación del sistema, generando incertidumbre de financiamiento. D11. No se ha definido la Interoperabilidad entre la Vertical de Salud y la ERP. D12. No se pueden conectar todos los ESM del SSFM, para poder tener el control total de la	D1-D4-O1: Fortalecer los cargos de planta del área y grupos para mejorar la gestión del conocimiento. D8-O1: Contratar personal capacitado para soportar la carga operacional de la administración de SALUD. SIS. D2-D6-D10-D17-D18-O3: Gestionar con el Ministerio de Defensa el financiamiento para la actualización de los equipos tecnológicos obsoletos que hacen parte de los sistemas de información. D3-D9-D13-D16-O2-O5: Realizar alianzas comerciales con proveedores exclusivos para el desarrollo e implementación de SALUD.SIS. D5-D7-D11-D12-D14-D15-O4-O6-O7-O8: Proponer que los planes nacionales y las políticas públicas este enfocadas en el fortalecimiento de una infraestructura segura que brinde integración e interoperabilidad de los sistemas de información del SSFM.	D2-D10-D17-D18-A2-A5: Presentar una estrategia en conjunto con el Ministerio donde se realice una adición en el presupuesto de salud nacional para contar con un adecuado financiamiento para la culminación del sistema. D5-D6-D7-D11-D13-D14-D15-A1-A2-A3: Evaluar integralmente la situación actual de la infraestructura, los equipos, la conectividad y las soluciones informáticas, entre otros, para poder impulsar una estrategia que priorice la inversión nacional en salud digital. D12-D16-A4: Ajustar el presupuesto general para dar prioridad a la implementación y uso de programas que garanticen la seguridad y privacidad de la información del SSFM.

información de manera integral y completa que nos dé la oportunidad de tomar decisiones únicas para todo el SSFM D13. Contar con proveedores exclusivos para el Desarrollo e Implementación de SALUD.SIS, lo que implica que podemos incurrir en sobrecostos. D14. Se necesita un ERP compatible con la Vertical de Salud para integrar y automatizar los procesos. D15. Falta interconectar los equipos Biomédicos con SALUD.SIS. D16. Que no se asegure la contratación continua de un Datacenter para el almacenamiento de la información. D17. No se cuenta con la financiación de los costos fijos de funcionamiento de SALUD.SIS. D18. No se cuenta con el Módulo de Facturación en el proyecto de SALUD.SIS		

9.1.5. Servicios de TI

La gestión de servicios de tecnologías de la información está basada en procesos, enfocada en alinear los servicios proporcionados en las necesidades de la Entidad, con énfasis en los beneficios que pueden percibir los usuarios.

A continuación, se nombran algunos servicios que ofrece el Grupo SISAM de la entidad:

Tabla 5. Servicios SISAM

SERVICIOS	DESCRIPCIÓN
Puestos de Trabajo	Suministro componentes informáticos requeridos para un puesto de trabajo: CPU, monitor, mouse, teclado, punto de red, Scanner, teléfono, extensión, Correo, licencias, carpetas compartidas, usuario de Red y reporte de daños presentado en los equipos.
Office 365	Conjunto de aplicativos ofimáticos que apoyan la ejecución de labores diarias, entre ellas están: Paquete office (Excel, Word, power point, one note) Microsoft Team, One drive, SharePoint. Azure Connection-colección de servidores y hardware de red).
Aplicativos misionales	Salud SIS
Aplicativos de Apoyo	Kactus, On base y visual médica.
Aplicativos de Servicio	Plataforma seguridad (Palo Alto) - Cortex XDR – mesa de servicio GLTI
Software de Terceros	GLPI- software libre de mesa de servicio. SGEDA- proporcionada por COMANDO

SERVICIOS	DESCRIPCIÓN
	SUITE VISION EMPRESARIAL-proporcionada por COMANDO
Internet E Intranet	GLOBAL PROTECH VPN - conexión de acceso Remoto que establece la conexión protegida del Usuario final a la red pública de la DIGSA. Wifi. Canales de Comunicación. Permisos de navegación -DIRECTORIO ACTIVO Creación de roles, usuario y contraseña-DIRECTORIO ACTIVO
Impresión	Servicio de impresión se presta por un tercero (Solución Copy)

Fuente: Elaboración propia SISAM

Los servicios de TI están definidos a través del Catálogo de Servicios TI y se pueden solicitar a través de la Mesa de ayuda, la ficha técnica asociada al Dominio de Arquitectura de Servicios Tecnológicos es la siguiente:

Tabla 6. Ficha Técnica Salud.SIS

Atributo	Descripción	
Nombre del sistema	SALUD.SIS	
Fuerza / dependencia del COGFM	Dirección General de Sanidad Militar	
Sigla	SALUD.SIS	
Descripción del sistema	Sistema de Información en Salud de las Fuerzas Militares	
Versión	1.0	
Categoría	Misional	X
	De apoyo	
	De Direccionamiento Estratégico.	
Tipo de desarrollo	Desarrollo Interno	X
	Desarrollo Externo	
	Adquirido sin modificaciones	
	Adquirido con modificaciones	
	Software como servicio	
Fabricante	Codaltec, UT Growtic de Salud S.A.S	
Proveedor de soporte	Growdata S.A.S.	
Fecha de vencimiento del soporte	31/12/2022	
Responsable Técnico	Gerente Proyecto SALUD.SIS - DIGSA	
Responsable Funcional	Líderes Funcionales DIGSA	
Estado	Activo (El sistema se encuentra en producción)	X
	Inactivo (El sistema ya no está en uso)	
	En desarrollo (El sistema está siendo construido o modificado)	X
Licenciamiento	Desarrollo Interno y propietario de DIGSA	
Sistema Operativo	Windows – Linux - Oracle	
Lenguaje de programación	Microsoft .NET Framework	
Plataforma de Base de Datos	Oracle 12c R2	
Documentación técnica y funcional	Documentación de manuales impresa y en repositorio de DIGSA	
Arquitectura Funcional	Web	

Fuente: Elaboración propia SISAM

Tabla 7. Ficha Técnica KACTUS

Atributo	Descripción	
Nombre del sistema	KACTUS-HCM	
Fuerza / dependencia del COGFM	Dirección General de Sanidad Militar	
Sigla	KACTUS	
Descripción del sistema	Sistema de Información de Recursos Humanos y Nómina	
Versión	12,6	
Categoría	Misional	
	De apoyo	X
	De Direccionamiento Estratégico.	
Tipo de desarrollo	Desarrollo Interno	
	Desarrollo Externo	X
	Adquirido sin modificaciones	
	Adquirido con modificaciones	
	Software como servicio	
Fabricante	DigitalWare S.A	
Proveedor de soporte	DigitalWare S.A	
Fecha de vencimiento del soporte	31/12/2023	
Responsable Técnico	Supervisor Técnico del contrato de soporte por parte de DIGSA	
Responsable Funcional	Supervisor Funcional del contrato de soporte por parte de DIGSA	
Estado	Activo (El sistema se encuentra en producción)	X
	Inactivo (El sistema ya no está en uso)	
	En desarrollo (El sistema está siendo construido o modificado)	
Licenciamiento	Desarrollo Externo y de propiedad de DIGSA	
Sistema Operativo	Windows Server 2019	
Lenguaje de programación	Delphi X3	
Plataforma de Base de Datos	Microsoft SQL Server 2017 Versión 18.6	
Documentación técnica y funcional	Documentación de manuales impresa y en repositorio de DIGSA	
Arquitectura Funcional	Web 80% - Cliente Servidor 20%	

Fuente: Elaboración propia SISAM

Tabla 8. Ficha Técnica OnBase

Atributo	Descripción	
Nombre del sistema	OnBase	
Fuerza / dependencia del COGFM	Dirección General de Sanidad Militar	
Sigla	OnBase	
Descripción del sistema	Software de gestión y control documental	
Versión	21,1,18,1000	
Categoría	Misional	
	De apoyo	X
	De Direccionamiento Estratégico.	
Tipo de desarrollo	Desarrollo Interno	

Atributo	Descripción	
	Desarrollo Externo	X
	Adquirido sin modificaciones	
	Adquirido con modificaciones	
	Software como servicio	
Fabricante	Hyland Software	
Proveedor de soporte	Giga de Colombia S.A.S.	
Fecha de vencimiento del soporte	31/12/2023	
Responsable Técnico	Supervisor Técnico del contrato de soporte por parte de DIGSA	
Responsable Funcional	Área Talento Humano DIGSA	
Estado	Activo (El sistema se encuentra en producción)	X
	Inactivo (El sistema ya no está en uso)	
	En desarrollo (El sistema está siendo construido o modificado)	
Licenciamiento	Desarrollo Externo de propiedad de DIGSA	
Sistema Operativo	Windows Server 2019	
Lenguaje de programación	.Net	
Plataforma de Base de Datos	Microsoft SQL Server 2017 Versión 18.6	
Documentación técnica y funcional	Documentación de manuales impresa y en repositorio de DIGSA	
Arquitectura Funcional	Cliente Servidor	

Fuente: Elaboración propia SISAM

Tabla 9. Ficha Técnica Visual Medica PACS

Atributo	Descripción	
Nombre del sistema	Visual Medica PACS	
Fuerza / dependencia del COGFM	Dirección General de Sanidad Militar	
Sigla	VM PACS	
Descripción del sistema	Software de almacenamiento, visualización, informes y distribución de Estudios Radiológicos	
Versión		
Categoría	Misional	
	De apoyo	X
	De Direccionamiento Estratégico.	
Tipo de desarrollo	Desarrollo Interno	
	Desarrollo Externo	X
	Adquirido sin modificaciones	
	Adquirido con modificaciones	
	Software como servicio	
Fabricante	Visual Médica	
Proveedor de soporte	Servidiagnostics S.A.S.	
Fecha de vencimiento del soporte	31/12/2023	
Responsable Técnico	Supervisor Técnico del contrato de soporte por parte de DIGSA	
Responsable Funcional	Líder Funcional Apoyo Diagnóstico SALUD.SIS	
Estado	Activo (El sistema se encuentra en producción)	X

Atributo	Descripción	
	Inactivo (El sistema ya no está en uso)	
	En desarrollo (El sistema está siendo construido o modificado)	
Licenciamiento	Desarrollo Externo de propiedad de DIGSA	
Sistema Operativo	Windows Server 2019	
Lenguaje de programación	.Net	
Plataforma de Base de Datos	Microsoft SQL Server 2017 Versión 18.6	
Documentación técnica y funcional	Documentación de manuales impresa y en repositorio de DIGSA	
Arquitectura Funcional	Web	

Tabla 10. Ficha Técnica SAP

Atributo	Descripción	
Nombre del sistema	Systems Applications and Products in Data Processing (SAP SE)	
Fuerza / dependencia del COGFM	Dirección General de Sanidad Militar	
Sigla	SAP	
Descripción del sistema	ERP (Planificación de recursos empresariales) software basado en la web y servicios basados en la actividad empresarial	
Versión	7.70	
Categoría	Misional	
	De apoyo	X
	De Direccionamiento Estratégico.	
Tipo de desarrollo	Desarrollo Interno	
	Desarrollo Externo	X
	Adquirido sin modificaciones	
	Adquirido con modificaciones	
	Software como servicio	
Fabricante	SAP	
Proveedor de soporte	SILOG	
Fecha de vencimiento del soporte	Diciembre 2023	
Responsable Técnico	Supervisor Técnico del contrato de soporte por parte de DIGSA	
Responsable Funcional	Área de SISAM	
Estado	Activo (El sistema se encuentra en producción)	X
	Inactivo (El sistema ya no está en uso)	
	En desarrollo (El sistema está siendo construido o modificado)	
Licenciamiento	Desarrollo Externo de propiedad de DIGSA	
Sistema Operativo	Windows Server 2019	
Lenguaje de programación	ABAP	
Plataforma de Base de Datos	SAP HANA	
Documentación técnica y funcional	Documentación de manuales impresa y en repositorio de DIGSA	
Arquitectura Funcional	Web	

Fuente: Elaboración propia SISAM

9.1.6. Políticas y estándares para la gestión de la gobernabilidad de TI

Tabla 10. Políticas y estándares para la gestión de la gobernabilidad de TI

Política	Descripción
Seguridad	La DIGSA cuenta con el apoyo del Comando General para el manejo de la seguridad de la información. Adicionalmente cuenta con procesos de seguridad de información en los sistemas de información que maneja, lo mismo que el compromiso de confidencialidad de los funcionarios que laboran en el Subsistema de Salud de las Fuerzas Militares.
Continuidad del negocio	A la fecha se encuentra en funcionamiento SALUD.SIS, que garantiza el registro de la historia clínica y la expedición de las órdenes de servicio y fórmula médica, adicionalmente maneja en tiempo real las afiliaciones y recaudo de los aportes de los afiliados al Subsistema de Salud de las Fuerzas Militares. El manejo del Fondo Cuenta se maneja a través del ERP de SAP, no se encuentran integrados estos sistemas.
Gestión de la Información	Se administra a través del proceso Gestión de la Información el cual Garantiza un adecuado flujo de información en todos los Niveles del SSFM, permitiendo a la Dirección General de Sanidad Militar desarrollar nuevas capacidades administrativas, identificar los grupos de valor o partes interesadas y controlar los canales de información.
Desarrollo de Sistemas de Información	A la fecha se cuenta con los módulos que hacen parte del Sistema de Información SALUD.SIS, lo mismo que la integración con nuestros procesos de apoyo (administrativos, logísticos y financieros). Estado actual de los módulos salud sis -

Fuente: Elaboración propia GRUGI

9.1.7. Capacidades de TI

A continuación, se relacionan las Capacidades de TI que hacen parte de la gestión de las Tecnologías de la Información de la Entidad.

Tabla 11. Capacidades de TI

Categoría	Capacidad	Cuenta con la Capacidad en la Entidad
Estrategia	Gestionar arquitectura empresarial	NO
	Gestionar Proyectos de TI	SI
	Definir políticas de TI	NO
Gobierno	Gestionar Procesos de TI	SI
Información	Administrar modelos de datos	SI
	Gestionar flujos de información	SI
Sistemas de Información	Definir arquitectura de Sistemas de Información	SI
	Administrar Sistemas de Información	SI
	Interoperar	NO
Infraestructura	Gestionar disponibilidad	SI
	Realizar soporte a usuarios	SI
	Gestionar cambios	NO
	Administrar infraestructura tecnológica	SI
Uso y apropiación	Apropiar TI	SI
Seguridad	Gestionar seguridad de la información	SI

Fuente: Elaboración propia GRUGI

9.1.8. Tablero de control de TI

La dirección no cuenta con un tablero de indicadores que permita tener una visión general del avance de la estrategia TI de la entidad y del sector.

9.2. Gobierno de TI

Las Tecnologías de Información y las Comunicaciones en la entidad se encuentra en construcción de un modelo administrativo de gobierno y gestión, que dé el direccionamiento y supervisión ejecutiva y además garantice el alineamiento, la planeación, organización, entrega de servicios de TI de manera oportuna, continua y segura.

9.2.1. Modelo de Gobierno de TI

9.2.1.1. Responsables

Definición de la instancia de Gobierno de TI, la toma de decisiones en lo relacionado con las TIC de la DIGSA se representa por una instancia de decisión que hace parte del Comité Directivo de la entidad, donde con periodicidad ANUAL se evaluará el desempeño de la gestión de las TIC en la entidad, se revisan los indicadores del tablero de control de TI y se toman decisiones de fortalecimiento a implementar y la prioridad de estas.

Los miembros que componen la instancia de decisión son:

- Director de la DIGSA ó un representante.
- Directores de Sanidad del Ejército Nacional, Armada de Colombia y la Jefatura de Salud de la Fuerza Aeroespacial Colombiana o sus representantes
- Los Subdirectores Administrativo y Financiero, de Salud y Subdirector Técnico y de Gestión o su representante
- Coordinador Grupo SISAM (Será el secretario del Comité) o su representante
- Gerente de Proyecto SALUD.SIS o su representante
- Coordinador Grupo Planeación Estratégica o su representante

De las sesiones de trabajo realizadas se lleva un registro de las ayudas de memoria de las reuniones, decisiones tomadas y compromisos acordados.

9.2.1.2. Mapa de Riesgos – Definición y gestión de la Matriz de Riesgos

Define los criterios básicos basándose en la Identificación de los activos de información, valoración de riesgos asociados a los activos de información de los procesos establecidos en el alcance del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. Así mismo el establecimiento y calificación de los controles para la obtención de los riesgos residuales de los procesos evaluados.

Tabla 12. Matriz de Riesgos

Mapa Riesgos Dirección General de Sanidad Militar

Análisis del riesgo inherente				Evaluación del riesgo - Valoración de los controles				Atributos						valuación del riesgo - Nivel del riesgo residu					
Criterios de impacto	Impacto Inherente	%	Zona de Riesgo Inherente	No. Control	Descripción del Control	Afectación	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento
Entre 100 y 500 SMLMV	Mayor	80%	Alto	1	El responsable de servidores realiza mensualmente la generación de un reporte con la herramienta LIVE OPTICS que permite conocer la capacidad de hardware del DATACENTER, con el fin de detectar saturación en los servicios y/o capacidad de recursos.	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	Media	50%	Mayor	80%	Alto	Reducir (mitigar)
				2	El responsable de FIREWALL realiza diariamente validaciones de vulnerabilidad en la red, realizando análisis, bloqueos, seguimiento, con el fin de prevenir ataque a la infraestructura tecnológica, frente a las acciones identificadas se realiza bloqueo a PUERTOS, URLS, DIRECCIONES IP. **Se genera un reporte mensualmente y se presenta al Coordinador del grupo de trabajo.**	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	Baja	25%	Mayor	80%	Alto	Reducir (mitigar)
Mayor a 500 SMLMV	Catastrófico	100%	Extremo	1	El responsable de FIREWALL realiza diariamente validaciones de vulnerabilidad en la red, realizando análisis, bloqueos, seguimiento, con el fin de prevenir ataque a la infraestructura tecnológica, frente a las acciones identificadas se realiza bloqueo a PUERTOS, URLS, DIRECCIONES IP. **Se genera un reporte mensualmente y se presenta al Coordinador del grupo de trabajo.**	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	Media	50%	Catastrófico	100%	Extremo	Reducir (mitigar)
				2	el responsable de Antivirus se realiza diariamente validaciones de bloqueos de amenazas presentadas mendiante la herramienta de solucion de seguridad CORTEX XDR, en equipos de los funcionarios y los servidores de la DIGSA.	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	Baja	25%	Catastrófico	100%	Extremo	Reducir (mitigar)
Mayor a 500 SMLMV	Catastrófico	100%	Extremo	1	El responsable de copias de seguridad realiza semestramental capacitación de copias de seguridad a los procesos y verifica mendiante seguimiento el cumpliento de los archivos generados, realizando pruebas de verficación de integridad de los datos. **Soporte Corte: El informe de capacitaciòn y/o informe seguimiento cumplimiento copias se seguridad.**	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	Media	50%	Catastrófico	100%	Extremo	Reducir (mitigar)
				2	El responsable de copias de seguridad de servidores realiza periodicamente las copias de respaldo de acuerdo al procedimeineto establecido y los planes de mantenimiento implementados en los manejadore de base de datos	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	Baja	25%	Catastrófico	100%	Extremo	
				1	El responsable de activacion de usuarios para el ingreso de Datacenter y cuartos electricos mediante la aplicación Bio star 2, siguiendo la debida autorizacion de la coordinacion de SISAM. **se genera un reporte de las novedades mensualmente y se presenta al Coordinador del grupo de**	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	Media	60%	Catastrófico	100%	Extremo	Reducir (mitigar)
				2	El responsable autorizado Diligencia la bitacora de ingreso al datacenter con las actividades realizadas, fecha, hora de entrada y de salida, firma y nombre del la persona de quien lo acompaña si aplica.													

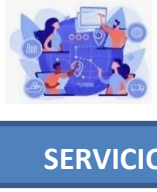
9.2.1.3. Gestión y Supervisión del Presupuesto funcionamiento y/ó Inversión

Los gastos de funcionamiento son recursos que se asignan de manera anual a la DIGSA y obedecen a una previa programación de necesidades que se realiza con un año de anticipación tendiente a sostener las capacidades de la Entidad en el mejor estado. La planeación obedece a la recolección de las necesidades que son recibidas de cada Dirección de Sanidad, Jefatura Salud y dependencia de la DIGSA de acuerdo con su competencia, se realiza la depuración de dichas necesidades y se presenta un plan de compras que es revisado por el Gobierno Corporativo y depurado de acuerdo con los topes que establece la DIGSA en cuestión de dineros asignados para cada Dirección de Sanidad, Jefatura Salud y dependencia.

Tabla 12. Gestión financiera de TI 2023

DESCRIPCIÓN	VALOR HADWARE ($)	VALOR SOFTWARE ($)	VALOR SERVICIO ($)
Computador	240,000,000		
Discos Duros	20,000,000		
Access Point	10,000,000		
Sistema de Backup		170,000,000	
Licencia adobe create cloud para el área de comunicaciones estratégicas -licenciamiento de suite adobe acrobat pro-licencia adobe stock		20,000,000	
Licenciamiento antivirus por un año DIGSA endpoint + correo electrónico.		150,000,000	
Soporte de firewall Palo Alto		200,000,000	
Mantenimiento licencias SAP		510,028,532	
Suscripción Office 365		529,500,000	
Licenciamiento renovación sistema operativo DataCenter.		100,000,000	
Transformación Digital en Salud			150,000,000
Canales dedicados y conexión a internet - Fortaleza			200,000,000
Servicio de mantenimiento de infraestructura tecnológica			400,000,000
Licenciamiento, soporte y mantenimiento kactus-modulo smart people.			60,000,000
Continuidad del negocio- servicios en la nube +licencias de vimware			350,000,000
Hosting y mantenimiento página web DIGSA por un año. - en comunicaciones			150,000,000
Servicio de conmutador telefónico.			166,000,000
Licenciamiento, soporte sistema OnBase			150,000,000

Fuente: Elaboración propia SISAM



9.2.1.4. Gestión de asignación de Recursos Humanos

Aunque se acaba de surtir la incorporación a la planta de personal de los funcionarios de carrera administrativa, no se logró reclutar personal con el perfil necesitado en una oficina de tecnologías de la información el cual se encuentra conformado de la siguiente manera:

Tabla 13. Recurso humano SISAM -SALUS SIS

Personal ingenieros			
No.	Grado	Nombres y apellidos	Profesión
1	CR	José Mauricio Barrera Barrera	Gerente de proyecto SALUD.SIS
2	TC	Elizabeth Bocarejo Bautista	Coordinadora SISAM
3	SP	Rubio Castro Toledo	Sargento primero
4	SS	Andrés Antonio López López	Sargento Segundo
5	PD	Juan Orlando Ramos Valbuena	Ingeniero de Sistemas
6	PD	Roberto Rodríguez Perdomo	Ingeniero de Sistemas
7	TASD	Maryori Tatiana Leiva Ubillus	Tecnóloga Ambiental
8	TASD	Yamile López	Administradora de Empresa
9	TASD	Cristian Camilo Rodríguez Delgado	Administrador Publico
10	AASD	Gustavo Adolfo Torres Forero	Ingeniero de Sistemas
11	AASD	Linda Jasbleidy Rodríguez Vásquez	Tecnóloga en Gestión de Redes de Datos
12	OPS	Néstor Andrés Gómez Gómez	Ingeniero Electrónico - Especialista Power BI
13	OPS	Lozano Arboleda Ramiro	Ingeniero de Sistemas
14	OPS	Karen Tatiana Rojas Rodríguez	Gestor Documental (secretaria)
15	OPS	Ingrid Mileyda Martínez Guevara	SALUD.SIS
16	OPS	Mary Elsy Castañeda Urbano	SALUD.SIS
17	OPS	Irlene Flores Vertel	SALUD.SIS

Fuente: Elaboración propia SISAM

9.2.2. Esquema de Gobierno de TI

La Dirección General de Sanidad Militar, la Subdirección Técnica y de Gestión y el Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, muestra su organización para el Gobierno Digital, teniendo en cuenta la organización y funciones definidas en la Resolución 0322 del 03 de abril de 2020, de la siguiente forma:

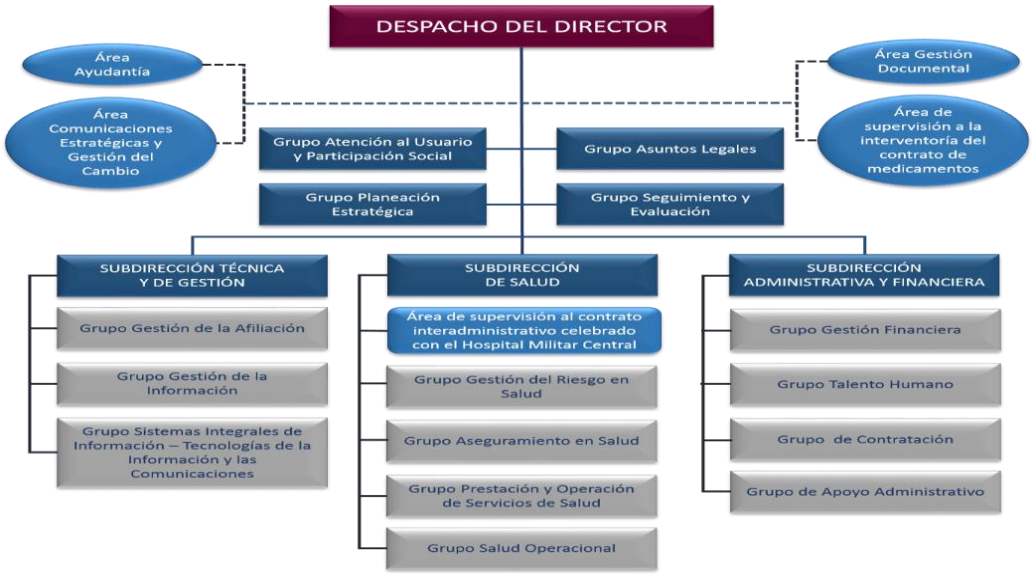


Ilustración 4. Esquema de Gobierno DIGSA

En forma detallada se presenta la estructura de la Subdirección Técnica y de Gestión, que es el enlace con el Despacho del Director para el Grupo Sistema Integral de Información-Tecnologías de Información y las Comunicaciones.

Ilustración 5. Organigrama SUBTG

El área de TI se detalla en la estructura del Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones:

Ilustración 6. Gobierno Digital SISAM

9.2.3. Gestión de Proyectos de TI

- Todos los proyectos de tecnología de la información y comunicaciones son viabilizados inicialmente por el Comité de integración de tecnologías de Información (CITI), utilizando la metodología que cuenta para este propósito.

- Cuando son proyectos de inversión estos son inscritos en el Banco de Programas y Proyectos (BPIN) del Departamento Nacional de Planeación (DNP) bajo la metodología MGA y luego son viabilizados año a año en los Comités Funcionales.

- Para todos los procesos de contratación se define de manera integral y completa las actividades necesarias para evaluar los aspectos legales asociados a un proyecto, desde su estructuración, estudio de viabilidad, contratación y cierre.

9.3. Gestión de Información

9.3.1. Arquitectura de Información

La estructura con la cual está representada y almacenada la información de la DIGSA, lo mismo que los servicios y los flujos de información, incluye el modelo conceptual, el modelo de indicadores, los componentes de información y sus relaciones, y la representación lógica y física de los datos, entre otros. En el gráfico se muestran las diferentes instancias para poder contar con una herramienta de toma de decisiones.

A la fecha la entidad cuenta con varias fuentes de información que no se cuentan integradas entre sí, generando inconvenientes a la hora de tomar decisiones por no contar con información unificada.

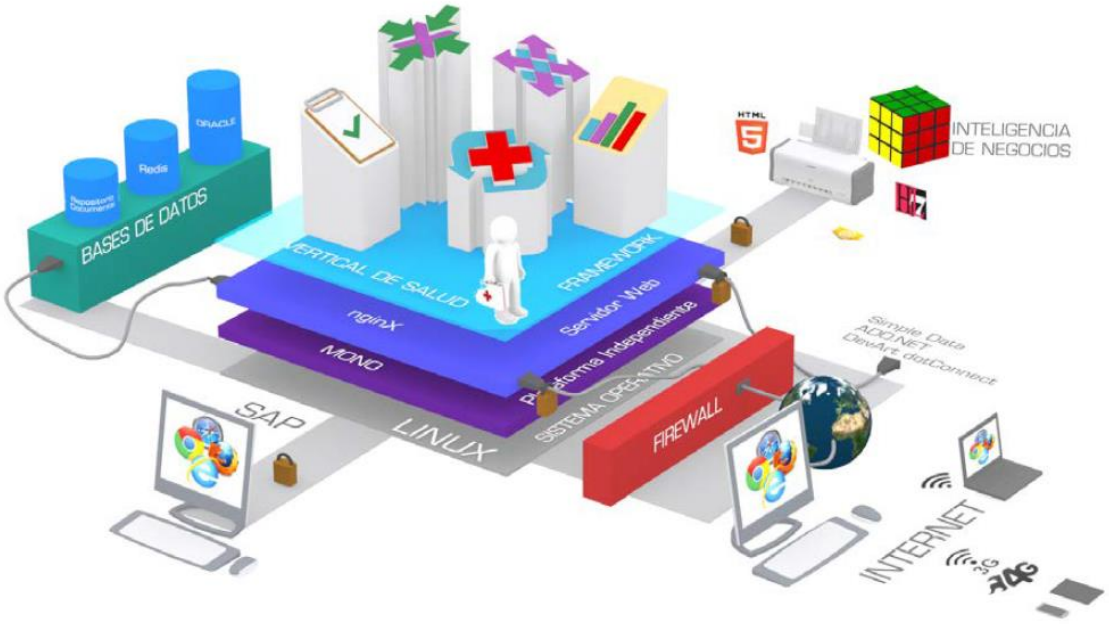


Ilustración 7. Modelo de Gestión de la Información SALUD.SIS

9.3.2. Gestión de la calidad y seguridad de la información

Actualmente se tienen sistemas de información que están desarrollados en diferentes herramientas y no cuentan con ambientes de desarrollo y calidad que permitan realizar el control de cambios sin afectar el ambiente productivo.

Así mismo la información almacenada en las bases de datos de los sistemas de información no cuentan con un alto nivel de calidad, para lo cual se proyecta implementar la analítica de datos que coadyuve al modelamiento de resultados asistenciales, mejoramiento en las decisiones y desarrollo de proyecciones.

9.3.3. Análisis y Aprovechamiento de los Componentes de información

Se está construyendo una herramienta de inteligencia de negocios que sirve de análisis para cada uno de los componentes de información con que se cuenta a través de los flujos de información de cada uno de los procesos de la entidad.

Desarrollo de capacidades para el uso de la información: La DIGSA mantiene la administración de datos maestros en alineación con el Sistema Integral de Información SALUD.SIS, cualquier proyecto que emprenda el Subsistema de Salud de las Fuerzas Militares en materia de

Sistemas de información institucional debe estar alineado con esta política y sus lineamientos derivados, por lo tanto, es deber de los interesados gestionar la comunicación con las áreas directamente encargadas de esta política basados en este documento.

Teniendo en cuenta el ámbito del dato se debe tener presente lo siguiente:

- El dato generado por la DIGSA es de índole público

  El intercambio de datos abiertos e interoperabilidad permitirá dar cumplimiento al dato generado por medio de: Acceso a los Datos, Ley de Transparencia, Apertura de Datos e Interoperabilidad de Datos, siguiendo las políticas de confidencialidad teniendo en cuenta que es información sensible.

  Por lo tanto, la DIGSA publica su información pública en el portal de datos abiertos del estado, esta actividad estará coordinada y es responsabilidad del Área de Comunicaciones Estratégicas y Gestión del Cambio.

- Los datos se producen bajo atributos de calidad

  Todos los datos e información que produzca la DIGSA se realizarán bajo procesos que respondan con los atributos de calidad de la administración de datos maestros, ciclo de vida de los datos, mapa de información, migración y procesos de calidad de la información.

  Como resultado de la gestión de la información se obtienen mecanismos de usos y accesos disponibles, información de calidad, generación de valor a partir de la información, apoyo a la toma de decisiones e instrumentos de análisis de la información disponible para los usuarios de la Dirección General de Sanidad Militar (DIGSA).

9.4. Sistemas de información

Como su nombre lo indica, va dirigido en primera instancia a los desarrolladores de software para que puedan comprender técnicamente, pero de manera simple, cuál es la arquitectura de software ideada para el Sistema de Información de Salud de las Fuerzas Militares.

Esto se aprecia en el diagrama de aplicaciones (ilustración 8), el cual abarca todas las decisiones y opciones que se tendrán para desarrollar cualquier módulo funcional en cualquiera de las fases de la solución de la vertical de salud, ya que expone de manera genérica los modelos aplicados.

Desde el Cliente se consume la aplicación web del servidor, es la primera parte de la distribución cliente-servidor. El cliente puede ser un navegador web o algún sistema externo a la aplicación de la vertical de salud. En el caso de un navegador web, se pueden manejar dos estilos de interfaces gráficas, MVC y SPA. En el estilo o patrón MVC, un usuario de la aplicación navega a través de ella siguiendo un flujo de trabajo paso a paso que lo lleva de una vista (página web en HTML) a otra, lo que implica cargar nuevas vistas o recargarlas. En el caso de SPA, las vistas o páginas normalmente permanecen activas por más tiempo y son

mucho más interactivas, por lo que resultan ideales para implementar paneles de control y casos de uso similares.

9.4.1. Catálogo de los Sistemas de información

El dominio de Sistemas de Información propone que para soportar los procesos de direccionamiento estratégico, misionales y de apoyo en una organización, es importante contar con sistemas de información que se conviertan en fuente única de datos útiles para la toma de decisiones en todos los aspectos; que garanticen la calidad de la información, dispongan recursos de consulta a los públicos de interés, permitan la generación de transacciones desde los procesos que generan la información y que sean fáciles de mantener. Que sean escalables, interoperables, seguros, funcionales y sostenibles, tanto en lo financiero como en la parte técnica, el catálogo de los sistemas de información es el siguiente:

Tabla 14. Software Interno

Software	Plataforma	Compatible con 1Pv6
Kactus	Delphi	SI
ERP	SAP	SI
Vertical de salud SALUD.SIS	VISUAL.NET	SI
Sistema de gesti6n documental ONBASE	Sin información	NO
Página WEB (Micrositios)	PHP	SI
Correspondencia	Access 2010	SI
Profesionales en salud	PHP	SI

Fuente: Elaboración propia SISAM

Software externo con el que se interactúa

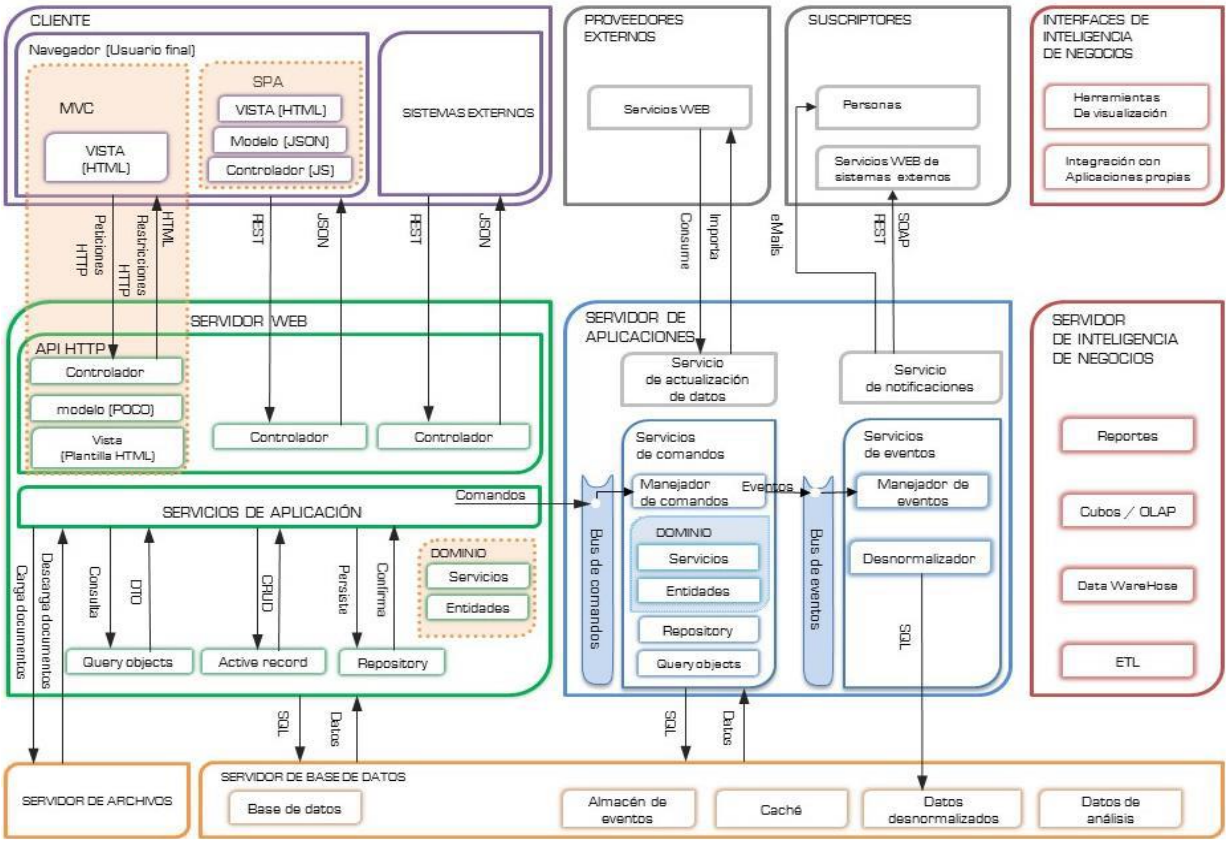
Tabla 15. Software Externos

Software	Plataforma	Compatible con 1Pv6
Siif nación	Visual.net	NA
Suite Visión	JSP	NA
Antivirus (Kaspersky)	Windows	NA
Correo electrónico (Outlook)	Windows	NA
Mesa de ayuda (msl)	Sin información	NA
Plataforma seguridad (palo alto)	Sin información	NA

Fuente: Elaboración propia SISAM

9.4.2. Mapa de Integraciones objetivo de sistemas de Información

Solo se tiene la integración de SALUD.SIS que se muestra a continuación:



Fuente: CDR CODALTEC

Ilustración 8. Integración de la aplicación Salud.SIS

9.4.3. Arquitectura de Referencia

La DIGSA cuenta con una infraestructura de servidores de los cuales unos se encuentran contratados y los otros tiene administración propia de la siguiente forma:

Tabla 16. Arquitectura de Referencia

Nombre de Dispositivo	Proveedor	Número dispositivos	Soporte IPV6	Documentación
Microsoft Virtual Wi-Fi Miniport Adapter	Microsoft	142	N/A	
Realtek PCIe GBE Family Controller	Realtek	98	SI	https://www.realtek.com/en/products/communications-network-ics/item/rtl8822bu
Dispositivo Bluetooth (Red de área personal)	Microsoft	93	N/A	
Bluetooth Device (Personal Área Network)	Microsoft	92	N/A	
Realtek 8822BU Wireless LAN 802.llac USB NIC	Semiconductor CORP	92	SI	https://www.realtek.com/en/products/ communications-network-ics/item/ rtl8822bu
Intel(R) Ethernet Connection I217-V	Intel Corporation	59	SI	https://www.intel.com/content/www/us/en/embedddatasheet.html?asset=9565
Intel(R) Wireless-N 7260	Intel	55	SI	
Intel(R) Ethernet Connection I217-V	Intel Corporation	43	SI	
Broadcom NetXtreme Gigabit Ethernet	Broadcom	39	SI	https://www.cnet.com/products/broadoom-netxtreme-ii-5709-network-adapter-
Intel(R) Dual Band Wireless-AC 3165	Intel Corporation	39	SI	https://fccid.io/YY3-1824VI/User-Manual/3165NGW-User-Manual-3357092

Nombre de Dispositivo	Proveedor	Número dispositivos	Soporte IPV6	Documentación
Intel(R) Ethernet Connection (5) 1219-LM	Intel	39	SI	ttp://www.intel.com/contentjwww/us/en/embedd
Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Client)	Broadcom Corporation	16	SI	https://www.cnet.com/products/broadcom-netxtreme-ii-5709-network-adapter-
HP NC553i Dual Port Flex Fabric 10Gb Converged Network Adapter	Emulex	16	SI	https://h20628.www2.hp.com/km-ext/kmcsdirect/emr_N/ A-a00042288en us-6.pdf
Intel(R) 82567LM-3 Gigabit Network Connection	Intel	13	SI	https://www.intel.com/content/www/us/en/support / articles/000026219/network-and-i-o.html
Conexi6n de red Gigabit Intel(R) 82567LM-3	Intel	12	SI	https://www.intel.com/contentjwww/us/en/support/ articles/000026219/network-and-i-o.html
Intel(R) Dual Band Wireless-AC 8260	Intel	12	SI	https://www.intel.com/contentjwww/us/en/product s/docs/wireless-products/dual-band-wireless-ac-8260-brief.html
Intel(R) Ethernet Connection I219-LM	Intel	12	SI	http://www.intel.com/content/www/us/en/embed d ed/products/networking/ethernet-connection-i219-datasheet.html
Gigabit Ethernet Broadcom	Broadcom	9	SI	https://www.cnet.com/products/broadoom-netxtreme-ii-5709-network-adapter-
HP NC382i DP Multifunction	Hewlett- Packard Company	8	SI	https://support.hpe.com/hpsc/ doc/public/display?d
Gigabit Server Adapter	Company			
HP NC553i Dual Port FlexFabric 10Gb Converged Network Adapter	ServerEngines Corporation	8	SI	https://h20628.www2.hp.com/km-
Broadcom BCM943228Z	Broadcom	7	SI	http://www8.hp.com/h20195/v2/GetPDF.aspx/ 4AA7
Intel(R) Ethernet Connection (2) 1219- LM	Intel	7	SI	http://www.intel.com/contentjwww/us/en/embed d
Intel(R) 82574L Gigabit Network Connection	Intel Corporation	5	SI	https://www.intel.com/contentjwww/us/en/embedd
TAP-Windows Provider V9	TAP-Windows Provider V9	5	N/A	https://www .cnet.com/products/broadcom-
Broadcom BCM5708C	Broadcom Corporation	4	SI	https://www.intel.com/contentjwww/us/en/embedd
Conexi6n de red Gigabit Intel(R) V82574L	Intel Corporation	4	SI	https://www.intel.com/contentjwww/us/en/embedd
Qualcomm Atheros QCA9565 802.llb/g/ n WiFi Adapter	Qualcomm Atheros Communication	4	SI	https://www.qualcomm.com/products/qca9377/documentation
Intel(R) PRO/1000 MT Network Connection	Intel	3	SI	https://downloadcenter.intel.com/ es/downloads/eula/28410/Gu-a-del-usuario-del-adaptador-de-Ethernet? http Down=https%3A %2F%2 Fdownloadmirror .intel.com%2F28410%2Feng%2FAdapter_User _ Guide.zip
Atheros AR9285 802.llb/g/n Wi-Fi Adapter	Atheros comunications Inc	2	N/A	
Fortinet SSL VPN Virtual Ethernet Adapter	Fortinet Inc.	2	N/A	
HP NC373i Multifunction Gigabit Server Adapter	Hewlett- Packard Company	2	SI	http://pdfstream.manualsonline.com/3/360eef48-6af6-4266-adca-f6031b562912.pdf
HP Network Teaming Virtual Miniport Driver	Hewlett- Packard Company	2	N/A	
PPPoP WAN Adapter	Fortinet Inc.	2	N/A	
VMware Virtual Ethernet Adapter for VMnetl	VMware, Inc.	2	N/A	
VMware Virtual Ethernet Adapter for VMnetl	VMware, Inc.	2	N/A	
Adaptador de red 1394	Microsoft	1	N/A	

Nombre de Dispositivo	Proveedor	Número dispositivos	Soporte IPV6	Documentación
Atheros AR9285Qualcomm Wireless Networt	Qualcomm Atheros Communications Inc	1	NO	
BASP Virtual Adapter	Broadcom	1	N/A	
Cisco Systems VPN	Cisco Systems	1	N/A	
Fortinet virtual Adapter	Fortinet	1	N/A	
Fortinet Virtual	Fortinet	1	N/A	
Intel(R) Centrino(R) Wireless-N 2230	Intel Corporation	1	SI	https://www.intel.com/contentjdam/www/public/us/en/documents/product-briefs/centrino-wireless-n- 2230-brief.pdf
Microsoft Wi-Fi	Microsoft	1	N/A	
Direct Virtual ADAPTER WLAN	Broadcom	1	SI	https://www.cnet.com/products/ dell-wireless-1397- network-adapter-4303166/
alámbrica Dell 1397 NIC de Gigabit Ethernet PCI-E	Realtek	1	N/A	
Qualcomm Atheros AR8152/8158 PCI-E Fast Ethernet Controller (	Qualcomm Atheros	1	N/A	
Realtek PCIe FE Family Controller	Realtek	1	N/A	
VirtualBox Host-Only Ethernet Adapter	Oracle Corporation	1	N/A	
VMware Accelerated AMD PCNet Adapter	VMware, Inc.	1	N/A	

Fuente: Información propia SISAM

Las comunicaciones se manejan a través de los siguientes enlaces:

Tabla 17. Comunicaciones TI

Marca	Descripción	Dual Stack	Dual Stack IPV6	Documentación
Palo Alto PA 3220	Firewall	SI	SI	https://media.paloaltonetworks.com/document
ARUBA 2930 F	SWITCH CORE	SI	SI	https://www.arubanetworks.com/assets/ds/DS 2930FSwitchSeries.pdf
3COM 5500 G	SWITCH	SI	SI	http://itclatam.com/pdf/3com5500.pdf
HP 2920	SWITCH	SI	SI	https://andovercg.com/datasheets/hp-2920- switches.pdf
CISCO800	SWITCH	SI	SI	https://www.cisco.com/c/en/us/products/collateral/routers/800m-integrated-services-router- isr/datasheet-c78-732678.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS 2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS 2930FSwitchSeries.pdf
ARUBA 2930F	SWITCH	SI	SI	https://www.arubanetworks.com/assets/d DS 2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS 2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
ARUBA 2930F	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS 2930FSwitchSeries.pdf

Marca	Descripción	Dual Stack	Dual Stack IPV6	Documentación
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
ARUBA 2930F	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf

Fuente: Información propia SISAM

9.4.4. Administración de la Operación

De acuerdo con los activos de TI se verificó el cumplimiento de la transición de la tecnología IPV4 a IPV6 el cual se encuentra administrado directamente por la DIGSA.

Los activos de TI que no aplican a la versión de IPV6 se hará el estudio correspondiente para comprobar su aplicabilidad o en su defecto dar de baja.

9.4.5. Mantenimiento de los Sistemas de información

Tabla 18. Mantenimiento de los Sistemas de Información

Actividad	Grado de madurez	Descripción hallazgo u oportunidad de mejora
Mantenimientos Preventivos	Implementado	Este mantenimiento está orientado a revisar, monitorear, estudiar y proponer soluciones a incidencias o inexactitudes en el sistema, basándose en la información recabada a partir de las tareas de análisis, revisión y monitoreo, se revisarán: - Errores descubiertos en SOFTWARE en productivo - Diagnostico a los errores descubiertos - Posible resolución de errores descubiertos
Mantenimientos Evolutivos	Implementado	Orientado al análisis, diseño, desarrollo y entrega de soluciones nuevas y necesarias para cubrir las actualizaciones o nuevas funcionalidades de los módulos en productivo del sistema. El mantenimiento evolutivo se elaborará: - Descripción requerimientos escalada al proveedor del servicio - Tiempo de resolución de los requerimientos escalados al proveedor - Descripción requerimientos solucionados - Descripción requerimientos rechazados - Relación de tiempo descontado de la bolsa por requerimiento - Porcentaje de avance por cada solución en desarrollo
Mantenimientos Correctivos	Implementado	En caso de mal funcionamiento, el proveedor efectuará mantenimiento correctivo, reingeniería de las funcionalidades, web service y/o componentes de software donde se presenten incidentes, fallas o errores, se revisarán: - El proveedor realizará diagnóstico del incidente o falla escalado por el comité de cambios de DIGSA - Hacer análisis de la solución y entregar el formato de control de cambios

Actividad	Grado de madurez	Descripción hallazgo u oportunidad de mejora
		- Hacer el diseño y desarrollo de la solución - Hacer pruebas de la solución en el entorno de pruebas, incluyendo pruebas unitarias e integrales debidamente documentadas y en coordinación con el comité de control de cambios

Fuente: Información propia SISAM

9.4.6. Soporte de los Sistemas de Información

Tabla 19. Soporte de los Sistemas de Información

Prioridad	Tiempo de respuesta	Descripciones de los niveles de servicios
1	2 horas (en horario 7*24)	"Caída del sistema" o situación del producto inoperativo que afecta al entorno de producción y la conectividad de la institución.
2	4 horas (en horario 7*24)	Situación con repercusiones importantes para el negocio que probablemente pone en peligro el entorno de producción. El o los Switches pueden funcionar, pero de forma muy limitada.
3	6 horas (en horario 7*24)	Situación con repercusiones poco importantes para el negocio con la mayoría de las funciones de el o los Switches están en funcionamiento. Sin embargo, puede ser necesaria algún tipo de estrategia para poder restaurar el servicio.
4	24 horas (en horario 7*24)	Problema o cuestión menor que no afecta al funcionamiento de la plataforma.

Fuente: Información propia SISAM

9.5. Infraestructura de TI

La DIGSA cuenta con un Datacenter donde se encuentra la plataforma tecnológica que soporta los sistemas de información administrativos y los servicios TIC; el cual cuenta con las condiciones mínimas de operación, para garantizar el acceso y la disponibilidad.

En la actualidad se cuenta con equipos de hiperconvergencia para manejar la administración de la infraestructura de TIC, a la fecha se han tenido entre otros los siguientes beneficios: Eficiencia de datos, movilidad, Escalabilidad y eficiencia, protección de datos, alta disponibilidad, eficiencia de costos, centralización de máquinas virtuales, simplificación del Data Center y reducción de costos de TCO (Costo Total de Propiedad).

9.5.1. Arquitectura de Infraestructura tecnológica

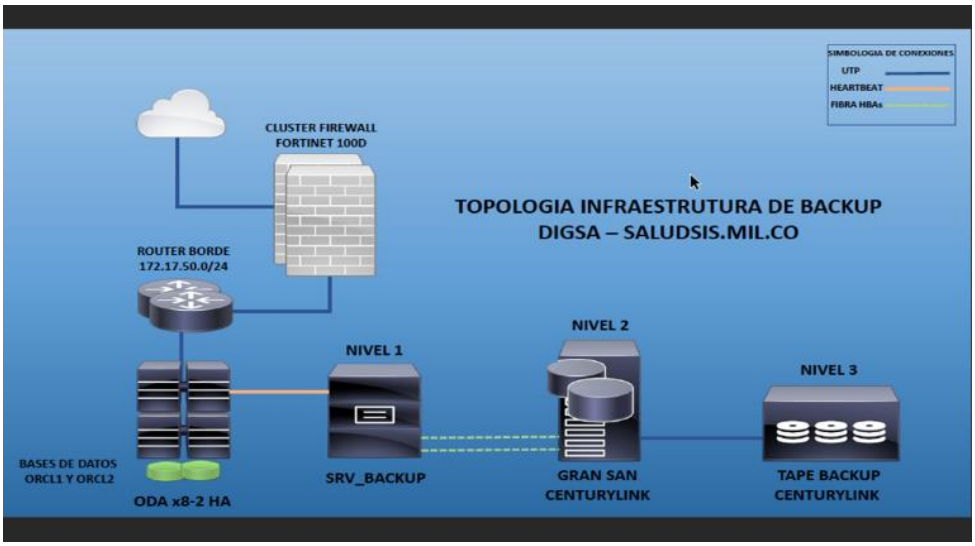


Ilustración 9. Arquitectura de TI

9.5.2. Administración de la capacidad de la infraestructura tecnológica

La DIGSA cuenta con una infraestructura de servidores de los cuales unos se encuentran contratados y los otros tiene administración propia de la siguiente forma:

Tabla 20. Capacidad de la Infraestructura Tecnológica

Nombre de Dispositivo	Proveedor	Número dispositivos	Soporte IPV6	Documentación
Microsoft Virtual WiFi Miniport Adapter	Microsoft	142	N/A	
Realtek PCIe GBE Family Controller	Realtek	98	SI	https://www.realtek.com/en/products/communications-network-ics/item/rtl8822bu
Dispositivo Bluetooth (Red de área personal)	Microsoft	93	N/A	
Bluetooth Device (Personal Área Network)	Microsoft	92	N/A	
Realtek 8822BU Wireless LAN 802.llac USB NIC	Semiconductor CORP	92	SI	https://www.realtek.com/en/products/ communications-network-ics/item/ rtl8822bu
Intel(R) Ethernet Connection I217-V	Intel Corporation	59	SI	https://www.intel.com/content/www/us/en/embedddata sheet.html?asset=9565
Intel(R) Wireless-N 7260	Intel	55	SI	
Intel(R) Ethernet Connection I217-V	Intel Corporation	43	SI	
Broadcom NetXtreme Gigabit Ethernet	Broadcom	39	SI	https://www.cnet.com/products/broadoom-netxtreme-ii-5709-network-adapter-
Intel(R) Dual Band Wireless-AC 3165	Intel Corporation	39	SI	https://fccid.io/YY3-1824VI/User-Manual/3165NGW-User-Manual-3357092
Intel(R) Ethernet Connection (5) 1219-LM	Intel	39	SI	ttp://www.intel.com/contentjwww/us/en/embedd
Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Client)	Broadcom Corporation	16	SI	https://www.cnet.com/products/broadcom-netxtreme-ii-5709-network-adapter-
HP NC553i Dual Port Flex Fabric 10Gb Converged Network Adapter	Emulex	16	SI	https://h20628.www2.hp.com/km-ext/kmcsdirect/emr_N/ A-a00042288en us-6.pdf
Intel(R) 82567LM-3 Gigabit Network Connection	Intel	13	SI	https://www.intel.com/content/www/us/en/support / articles/000026219/network-and-i-o.html

Nombre de Dispositivo	Proveedor	Número dispositivos	Soporte IPV6	Documentación
Conexi6n de red Gigabit Intel(R) 82567LM-3	Intel	12	SI	https://www.intel.com/contentjwww/us/en/support/articles/000026219/network-and-i-o.html
Intel(R) Dual Band Wireless-AC 8260	Intel	12	SI	https://www.intel.com/contentjwww/us/en/products/docs/wireless-products/dual-band-wireless-ac-8260-brief.html
Intel(R) Ethernet Connection I219-LM	Intel	12	SI	http://www.intel.com/content/www/us/en/embedded/products/networking/ethernet-connection-i219-datasheet.html
Gigabit Ethernet Broadcom	Broadcom	9	SI	https://www.cnet.com/products/broadoom-netxtreme-ii-5709-network-adapter-
HP NC382i DP Multifunction	Hewlett- Packard Company	8	SI	https://support.hpe.com/hpsc/ doc/public/display?d
Gigabit Server Adapter	Company			
HP NC553i Dual Port FlexFabric 10Gb Converged Network Adapter	ServerEngines Corporation	8	SI	https://h20628.www2.hp.com/km-
Broadcom BCM943228Z	Broadcom	7	SI	http://www8.hp.com/h20195/v2/GetPDF.aspx/ 4AA7
Intel(R) Ethernet Connection (2) 1219- LM	Intel	7	SI	http://www.intel.com/contentjwww/us/en/embedd
Intel(R) 82574L Gigabit Network Connection	Intel Corporation	5	SI	https://www.intel.com/contentjwww/us/en/embedd
TAP-Windows Provider V9	TAP-Windows Provider V9	5	N/A	https://www .cnet.com/products/broadcom-
Broadcom BCM5708C	Broadcom Corporation	4	SI	https://www.intel.com/contentjwww/us/en/embedd
Conexi6n de red Gigabit Intel(R) V82574L	Intel Corporation	4	SI	https://www.intel.com/contentjwww/us/en/embedd
	Broadcom Corporation	4	SI	https://downloadcenter.intel.com/es/downloads/eulEthernet>httpDown=https%3A%2F%2Fdownloadmirror.intel.com%2F28410%2Feng%2FAdapter User Guide.zip
Qualcomm Atheros QCA9565 802.llb/g/ n WiFi Adapter	Qualcomm Atheros Communication	4	SI	https://www.qualcomm.com/products/qca9377/documentation
Atheros AR9285 802.llb/g/n WiFi Adapter	Atheros comunications Inc	2	N/A	
Fortinet SSL VPN Virtual Ethernet Adapter	Fortinet Inc.	2	N/A	
HP NC373i Multifunction Gigabit Server Adapter	Hewlett- Packard Company	2	SI	http://pdfstream.manualsonline.com/3/360eef48-6af6-4266-adca-f6031b562912.pdf
HP Network Teaming Virtual Miniport Driver	Hewlett- Packard Company	2	N/A	
PPPoP WAN Adapter	Fortinet Inc.	2	N/A	
VMware Virtual Ethernet Adapter for VMnetl	VMware, Inc.	2	N/A	
VMware Virtual Ethernet Adapter for VMnetl	VMware, Inc.	2	N/A	
Adaptador de red 1394	Microsoft	1	N/A	
Atheros AR9285Qualcomm Wireless Networt	Qualcomm Atheros Communications Inc	1	NO	
BASP Virtual Adapter	Broadcom	1	N/A	
Cisco Systems VPN	Cisco Systems	1	N/A	
Fortinet virtual adapter	Fortinet	1	N/A	
Fortinet Virtual	Fortinet	1	N/A	
Intel(R) Centrino(R) Wireless-N 2230	Intel Corporation	1	SI	https://www.intel.com/contentjdam/www/public/us/en/documents/product-briefs/centrino-wireless-n- 2230-brief.pdf
Intel(R) Ethernet Connection I217-V	Intel Corporation	1	SI	https://www.intel.com/contentjwww/us/en/embedd ed/products/networking/i217-ethernet-controller-datasheet.html?asset=9565
Microsoft Wi-Fi	Microsoft	1	N/A	

Nombre de Dispositivo	Proveedor	Número dispositivos	Soporte IPV6	Documentación
Direct Virtual ADAPTER WLAN	Broadcom	1	SI	https://www.cnet.com/products/ dell-wireless-1397- network-adapter-4303166/
alámbrica Dell 1397 NIC de Gigabit Ethernet PCI-E	Realtek	1	N/A	
Qualcomm Atheros AR8152/8158 PCI-E Fast Ethernet Controller (	Qualcomm Atheros	1	N/A	
Realtek PCIe FE Family Controller	Realtek	1	N/A	
VirtualBox Host-Only Ethernet Adapter	Oracle Corporation	1	N/A	
VMware Accelerated AMD PCNet Adapter	VMware, Inc.	1	N/A	

Fuente: Información propia SISAM

Las comunicaciones se manejan a través de los siguientes enlaces:

Tabla 21. Comunicaciones de TI

Marca	Descripción	Dual Stack	Dual Stack IPV6	Documentación
Palo Alto PA 3220	Firewall	SI	SI	https://media.paloaltonetworks.com/document
ARUBA 2930 F	SWITCH CORE	SI	SI	https://www.arubanetworks.com/assets/ds/DS 2930FSwitchSeries.pdf
3COM 5500 G	SWITCH	SI	SI	http://itclatam.com/pdf/3com5500.pdf
HP 2920	SWITCH	SI	SI	https://andovercg.com/datasheets/hp-2920- switches.pdf
CISCO800	SWITCH	SI	SI	https://www.cisco.com/c/en/us/products/collateral/routers/800m-integrated-services-router- isr/datasheet-c78-732678.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS 2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS 2930FSwitchSeries.pdf
ARUBA 2930F	SWITCH	SI	SI	https://www.arubanetworks.com/assets/d DS 2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS 2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
ARUBA 2930F	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS 2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS 2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS 2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS 2930FSwitchSeries.pdf
HP 2920	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS 2930FSwitchSeries.pdf
ARUBA 2930F	SWITCH	SI	SI	https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf

Fuente: Información propia SISAM

9.5.3. Administración de la Operación

De acuerdo con los activos de TI se verificó el cumplimiento de la transición de la tecnología IPV4 a IPV6 el cual se encuentra administrado directamente por la DIGSA.

Los activos de TI que no aplican a la versión de IPV6 se realizó el estudio correspondiente para comprobar su aplicabilidad o en su defecto dar de baja.

9.6. Uso y Apropiación

De acuerdo con los resultados recolectados en la medición de uso y apropiación de los sistemas de información, se analizarán que medidas deben emplearse para eliminar las brechas que puedan generarse en la realización de las actividades laborales y asistenciales.

La Dirección General de Sanidad Militar a la fecha cuenta con el desarrollo del proyecto en productivo bajo la descripción de diferentes fases de la solución vertical de salud, los cuales se describen en la siguiente ilustración:

Ilustración 10. Módulos de vertical SaludSis

De los cuales ya se encuentran en productivo las funcionalidades básicas para que un Establecimiento de Sanidad Militar pueda manejarlo. Se tienen los siguientes indicadores, que muestran las bondades del sistema de información:

IMPLEMENTACIÓN			
FUERZA	SI	NO	
EJC	125	10	
FAC	23	0	
ARC	16	0	
TOTALES	164	10	174

% USABILIDAD	
FUERZA	%
EJC	*71,84%*
FAC	*13,22%*
ARC	*9,20%*
TOTALES	*94,25%*

- De los 174 ESM que existen, 164 Establecimientos de Sanidad Militar que están en productivo en la solución vertical de salud, tienen una usabilidad del 94,25% con una cobertura del 92.8% de un total de 667.725 Afiliados. Fuente SALUD.SIS

- Se tiene un registro de 14.617 usuarios activos en el Sistema, distribuidos entre la DIGSA, DISAN EJC, DISAN ARC, Jefatura Salud FAC y ESM. Quienes utilizan los componentes de: SALUD.SIS, ERP y SIIF NACION.

- Se han creado un total de 619.649 Historias Clínicas Electrónicas (92.8%), con lo cual se garantiza que sea integral y esté a disposición en línea a Nivel Nacional. Fuente SALUD.SIS

- Todos los procesos de recaudo se realizan con las Entidades Aportantes desde el módulo de SALUD.SIS.

9.6.1. Estrategia de Uso y Apropiación

En la DIGSA actualmente se adelantan actividades para fortalecer el talento digital y adopción de buenas prácticas de las herramientas de trabajo colaborativas (MINTIC) y de cuarta revolución industrial - 4RI, para mejorar la productividad, la toma de decisiones, la participación y la eficiencia en la prestación de los servicios. En seguida se hace un análisis de la situación actual desde los ámbitos de esta estrategia

Ámbito	Situación Actual
Estrategia para el Uso y la Apropiación	La Estrategia del Uso y la Apropiación de Tecnologías de Información, busca afianzar la cultura digital de los grupos de interés de la entidad y apoya la transformación digital que lidera el área de SISAM. Así mismo, se desarrollan actividades referentes a la movilización de los usuarios internos hacia la adopción de los proyectos de Tecnología de la Información y el desarrollo de competencias internas requeridas para aumentar las capacidades de Tecnologías de Información. El Plan de Transformación Digital (en realización actualmente) incluye un plan de formación para desarrollar competencias en la apropiación de tecnologías de 4RI que apoyan los procesos del ministerio de defensa e incluye las prácticas, procedimientos, recursos y herramientas necesarias
	A través de los tableros de control e indicadores para el monitoreo (POWER BI) y la evaluación de la estrategia del uso y la apropiación de Tecnologías de Información

Medición de Resultados de Uso y Apropiación	en la entidad, se establecen las acciones de mejora continua a partir de su análisis para fortalecer la cultura digital y satisfacer las necesidades de los usuarios.

A partir del ejercicio realizado por el equipo de transformación digital, se pudo establecer que a Junio – octubre 2023 el nivel de madurez digital en la DIGSA es 2, que corresponde a un nivel donde está en un proceso de INICIANDO se ha iniciado la transformación digital y se cuenta con iniciativas y un enfoque proactivo.

La siguiente ilustración muestra la valoración en cada una de las dimensiones que se cuantifican mediante la herramienta de medición y priorización Digital Shift suministrada por MinTIC. En ella se evidencia la evaluación actual que en materia de transformación digital ha iniciado la DIGSA en esta vigencia.

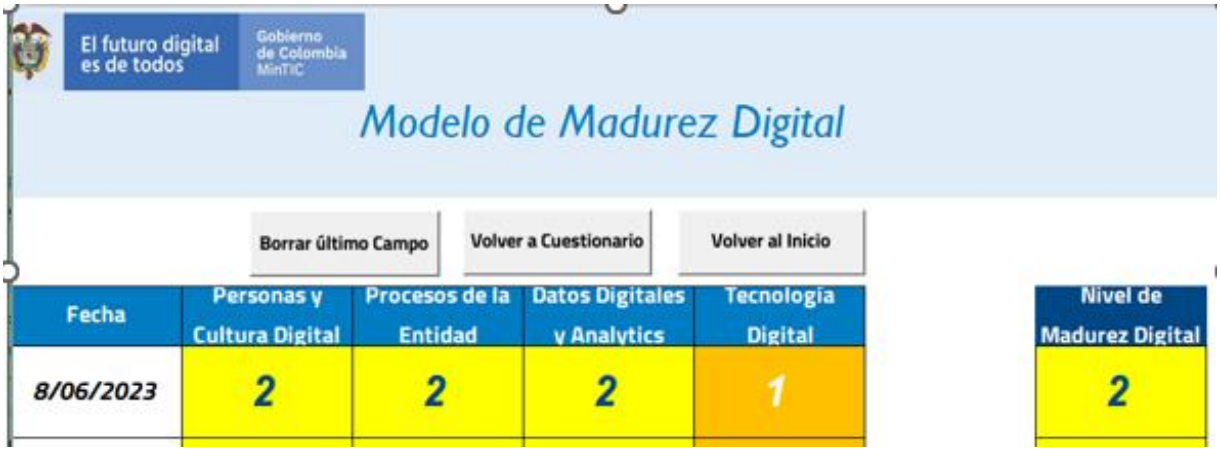


Ilustración 11 Modelo de madurez digital

9.6.2. Esquema de Incentivos

No existe ningún esquema de incentivos.

9.6.3. Plan de Formación

No existe un plan de formación formal, solo capacitaciones esporádicas.

9.6.4. Evaluación del nivel de adopción de TI

No existe evaluación de las Tecnologías de información.

9.6.5. Plan de capacitación y entrenamiento para los sistemas de información

No existe plan de capacitación ni entrenamiento, solo capacitaciones puntuales.

9.7. Seguridad

Se definirán las actividades a cumplir durante la presente vigencia para avanzar en la implementación del Sistema de Gestión de Seguridad de la Información de la Dirección General de Sanidad Militar, aplica a todos los activos de información que manejan los procesos misionales y el proceso de apoyo relacionado con la Gestión de Tecnología, conforme a lo establecido en el mapa de procesos y es de obligatorio cumplimiento por parte de todos los funcionarios, contratistas y terceras partes que presten sus servicios a la Dirección General de Sanidad Militar.

La implementación del Sistema de Gestión de Seguridad de la Información de las Direcciones de sanidad EJC, ARC, Y JEFSA, es gestionada a través de los Comandos de la respectiva Fuerza, quienes les proporcionan los servicios de infraestructura tecnológica.

9.7.1. Desarrollo del Plan de Seguridad de la Información

La metodología de implementación del Plan de Seguridad y Privacidad para la Dirección General de Sanidad Militar-DIGSA, está basado en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) y lo establecido en el Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, que contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que la DIGSA pueda gestionar adecuadamente la seguridad y privacidad de sus activos de información, así:

Ilustración 12. Ciclo de operación del Modelo de Seguridad de la Información

Teniendo en cuenta lo establecido en el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, la Dirección General de Sanidad Militar ha realizado las siguientes actividades:

9.7.1.1. Fase de Diagnostico Seguridad de la Información

- Se identificó el estado actual de madurez de la DIGSA con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.
- Se identificó el nivel de madurez del Modelo de Seguridad y Privacidad de la Información MSPI de la DIGSA de acuerdo con la herramienta de diagnóstico definida por MINTIC.

9.7.1.2. Fase de Planificación

- Se determinó el contexto en el que se establece el alcance que va a tener el Modelo de Seguridad y Privacidad de la Información de la DIGSA.

- Se definió la política general del Sistema de Gestión de Seguridad de la Información, la cual se encuentra firmada por el Señor Director General de Sanidad Militar y socializada al interior de la DIGSA.

- Se elaboró el Manual de Políticas de Seguridad y Privacidad de la Información.

- Se elaboraron los procedimientos de seguridad de la información.

- de las Infraestructuras Críticas Cibernéticas (ICC) y la clasificación de la información de los activos de información de la Dirección General de Sanidad Militar – DIGSA.

- Se realizó el plan de Sensibilización y Comunicación de seguridad de la información, dirigido a todos los funcionarios de la Dirección General de Sanidad Militar.

- Se verificó el cumplimiento de los controles de seguridad de la información implementados en la DIGSA.

9.7.1.3. Fase de Implementación

- Se elaboró la Declaración de Aplicabilidad que establece los controles y se actualizaron las políticas y procedimientos que está aplicando la DIGSA, basados en la norma ISO 27001:2013.

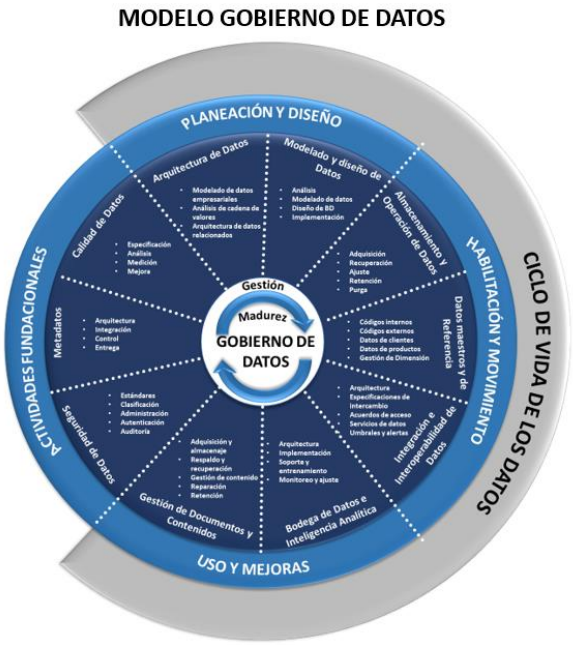
- Elaboración de los indicadores de gestión de seguridad de la información de la DIGSA.

- Se elaboró el plan institucional de seguridad y privacidad de la información en la DIGSA basado en la norma ISO/IEC/27001(2013).

10. SITUACIÓN OBJETIVO

Para definir el alcance y desarrollo d ellos modelos propuestas en esta sección del PETI, es indispensables contar con los productos de los dos Contratos que se están ejecutando actualmente en la DIGSA:

- Contrato Electrónico No. 144-DIGSA-2023, con objeto: Prestar los servicios profesionales como especialista en Gerencia y Calidad en Salud, para la modernización del SSFM, en el marco de la definición de la política de gobierno de datos de la Dirección General de Sanidad Militar, uno de los entregables es Diseñar la política de gobierno de datos del Subsistema de Salud de las Fuerzas Militares, Diseñar los componentes de la hoja de ruta, como base para el análisis de la brecha del Sistema de información SALUD.SIS, para la visión del gobierno de datos de la DIGSA. 4. Diseñar la hoja de ruta de la política de gobierno de datos (Alcance, inversión y recursos).



Fuente: Elaboración propia GRUGI – DIGSA 2023, adaptado DAMA Colombia

Ilustración *13.* Modelo de Gobierno de Datos DIGSA

Los mencionados entregables se recibirá por la Supervisión en septiembre del 2023, razón por la cual el PETI, se debe ajustar el enero del 2024, según estos y la ruta de

ejecución que se plantea, de igual forma el modelo propuesto en esta sección del PETI.

- Contrato Electrónico No. 168-DIGSA-2023, con objeto: Adquisición de servicios profesionales para la implementación del Modelo de Soporte Nivel II, Administración y Gobierno de la Plataforma Tecnológica, continuidad del negocio y Plan de Transformación Digital de la Dirección General de Sanidad Militar, uno de los entregables es el Diseño del Plan para la Transformación Digital en Salud de la DIGSA, incluye la estrategia de la transformación digital DIGSA, con su conjunto de proyectos y hoja de ruta de implementación. Entrega de informe detallado con cronograma de ejecución.

Fuente Mintic

Ilustración *13. Interacción Transformación Digital*

El mencionado entregable se recibirá por la Supervisión en diciembre del 2023, razón por la cual el PETI, se debe ajustar el enero del 2024, según este y la ruta de ejecución que se plantea, de igual forma el modelo propuesto en esta sección del PETI.

10.1. Tecnologías de Información y las Comunicaciones

Las Tecnologías de la Información y las Comunicaciones (TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes (Art. 6 Ley 1341 de 2009).

El Artículo 147 de la Ley 1955 del 2019 (Plan Nacional de Desarrollo) establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Así mismo, el CONPES 3975, que define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para

que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.

El Gobierno Nacional expide el Decreto 1389 del 28 de julio de 2022, "por el cual se adiciona el Título 24 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para la gobernanza en la infraestructura de datos y se crea el Modelo de gobernanza de la infraestructura de datos".

Este decreto tiene como propósito fortalecer la gobernanza en la infraestructura de datos, al permitir la articulación de actores, instancias, normas, entre otros, para implementar, gestionar y manejar la infraestructura de datos en Colombia, con el fin de crear valor público, social y económico a través de los datos.

10.1.1. Misión de TI

Adoptar y adaptar herramientas TIC como mecanismo de gestión de sistemas interoperables con datos abiertos que se utilizan éticamente, para generar información estratégica en beneficio de la salud de las fuerzas Militares.

Garantizar un adecuado flujo de información en todos los Niveles del SSFM, permitiendo a la Dirección General de Sanidad Militar desarrollar nuevas capacidades administrativas, identificar los grupos de valor o partes interesadas y controlar los canales de información.

10.1.2. Visión de TI

Garantizar el acceso y la cobertura nacional, fortalecidos mediante sistemas interconectados e interoperables que permita el acceso eficaz y eficiente a datos de calidad, información estratégica y herramientas de TIC para la toma de decisiones y el bienestar de los usuarios de las FFMM.

10.1.3. Objetivo estratégico de TI

Mejorar los servicios médicos, financieros, administrativos y jurídicos que garanticen el cumplimiento del derecho a la prestación de servicios de salud y bienestar de los afiliados y beneficiarios al Subsistema de Salud de las Fuerzas Militares a partir de las tecnologías de la información integrándolo en uno solo ecosistema de información a través de la arquitectura empresarial.

10.2. Productos modelo Gobierno TI

El Modelo de Gestión y Gobierno de TI (MGGTI) permitirá generar y actualizar las capacidades institucionales que se requieran para prestar servicios de TI a los usuarios de la Entidad, mediante el uso adecuado de las tecnologías de la información y las comunicaciones.

Los productos del MGGTI que se propone para actualizar las Tecnologías de la Información y las Comunicaciones, está compuesto por seis dominios que permiten alinear las necesidades del negocio mediante el uso adecuado de las TIC:

-Estrategia de TI,
-Gobierno de TI
-Gestión de Sistemas de Información,
-Gestión de Información,
-Gestión de Servicios de TI y
-Uso y Apropiación de TI.

Se explica cada producto a continuación:

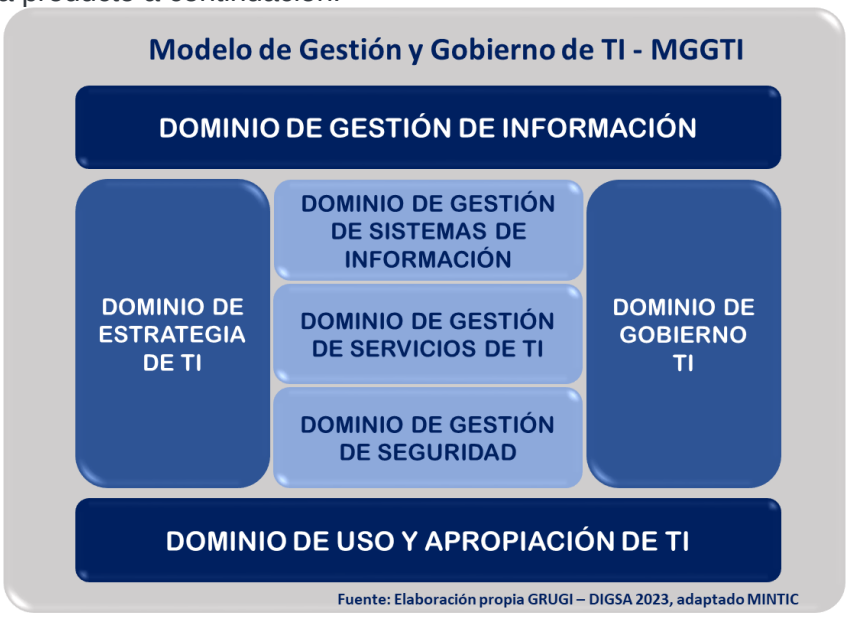


Ilustración 14. Modelo de Gestión y Gobierno

10.2.1. Estrategia de TI

Teniendo presente el marco normativo, la Dirección General de Sanidad Militar actualizará la Estrategia de Tecnologías de la Información, incluirá el Componente de Trasformación Digital, y la Política de Gobierno de Datos, como unos de los ejes fundamentales de la estrategia:

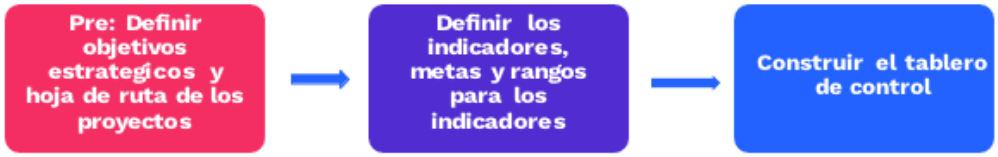
El Sistema Integral de Información en Salud del Subsistema de Salud de las Fuerzas Militares, como conjunto interrelacionado de usuarios, normas, procedimientos y recursos, que generen y dispongan información sobre los procesos esenciales de gestión de la afiliación, aseguramiento financiero, atención y prestación de servicios de salud , participación social y los procesos de gerencia y administración institucional, permitirá garantizar un adecuado flujo de información tanto interna como externa y la interacción con los usuarios y con otras entidades sectoriales, la operación y el desarrollo de sus funciones, la seguridad y protección de datos, la trazabilidad de la gestión y el control y evaluación; por lo cual se requiere desarrollar nuevas capacidades organizacionales y contar con canales de comunicación que hagan posible difundir y transmitir la información de calidad que se genera en toda la entidad, tanto entre dependencias como frente a los grupos de valor y partes interesadas.

Las nuevas capacidades permitirán la formación de los funcionarios de la Entidad en las herramientas de consolidación, presentación y análisis de la data mediante el uso de soluciones basada en inteligencia de negocios, permitiendo armonizar la gestión con los

estándares y metodologías modernas que el mercado ofrece, para el final de los proyectos, el personal tendrá las competencias para el manejo eficiente, efectivo y dinámico de la información, para el cumplimiento de la información ante los entes reguladores y el mercado externo.

10.2.2. Indicadores - Tableros de Control TI

En aprovechamiento de la información y uso de las herramientas disponibles para el análisis y visualización de la información, el área de SISAM está elaborando dashboards en power BI entre otras herramientas. A continuación, explicaremos algunos de los muchos proyectos que se encuentran en ejecución actualmente y durante el presente año se implementó el tablero de control de indicadores PETI el cual permite visualizar, de forma resumida, algunos de los indicadores predefinidos, los cuales pueden ser fácilmente adaptados por DIGSA para la medición de la estrategia de TI, gestión de TI y proyectos de TI.



a. Indicador tablero de control PETI

Actualmente se ejecutan cuatro indicadores del listado de indicadores propuestos por Mintic, Estos indicadores se ponderan y generan un único indicador, el cual se visualiza trimestralmente en la Suit visión Empresarial por seguimiento y control del PEI 2023

INDICADORES DIGSA								2023							
ID	TIPO DE INDICADOR	INDICADOR	%	FORMULA	VARIABLES	FRECUENCIA	RESPONSABLE	Enero	Febrero	Marzo	Abril	Mayo	Junio	CONSOLIDADO AÑO	INDICADOR
Indicador 1	Operación	Indice de disponibilidad de aplicativo WEB	ID	ID= (TSA-TB) /TSA*100)	TSA=Tiempo de servicio acordado TB= sumatorio de los tiempos sin servicio	TRIMESTRAL	COMUNICACIONES	99%	98%	99%	99%	99%	99%	99%	
Indicador 2	Operación	Indice de atención por canales electrónicos	IA	IA= (TTE-TT) *100)	TT= # total de tramites atendidos durante período TTE= # total de tramites atendidos por aplicativo web durante período	TRIMESTRAL	SERVICIO AL CLIENTE	91%	91%	91%	94%	94%	94%	93%	
Indicador 04	Operación	Cumplimiento en atención de requerimientos	ICR	ICR= (SAT / SR) *100)	SR= # de servicios requeridos en el periodo analizado SAT= # de servicios atendidos en el tiempo esperado durante el periodo analizado	TRIMESTRAL	AFILIACIONES	100%	100%	100%	100%	100%	100%	100%	
Indicador 9	Estratégicos	Variación en trámites atendidos	PAT	AT = (TA / NT) *100	NT: Total de trámites que tiene la entidad TA: Trámites Aprobados en la entidad.	TRIMESTRAL	AFILIACIONES	56%	55%	51%	52%	47%	51%	52%	
								95%	95%	95%	86%	85%	86%	95%	

Ilustración 15. Tablero de Control PETI

b. Tablero obsolescencia equipos de Cómputo.

Este tablero permite visualizar las novedades en equipos de cómputo en la DIGSA, tomando como fuente de información SAP.

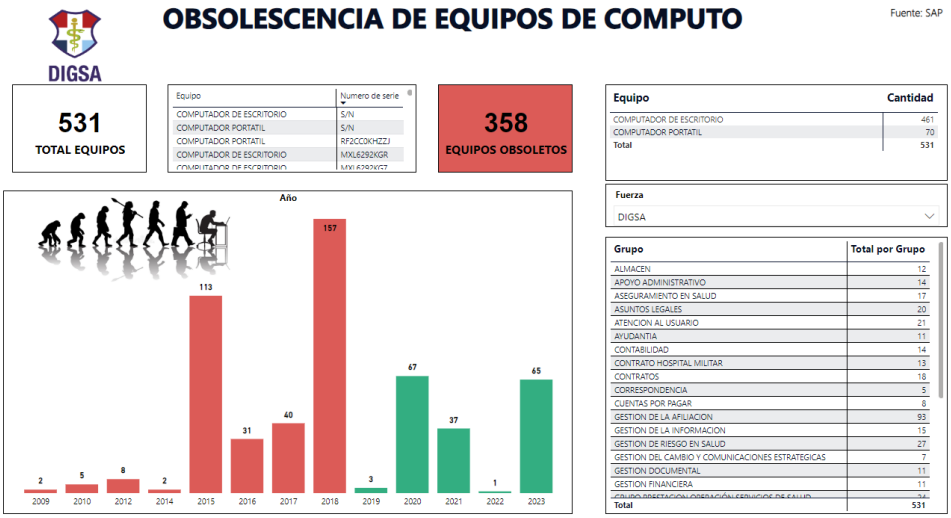


Ilustración *16.* Tablero Obsolescencia de Equipos

c. Tablero registro de llamadas

Este tablero permite visualizar el consolidado de llamadas que ingresan a línea institucional de la DIGSA, tomando fuente base estructurada

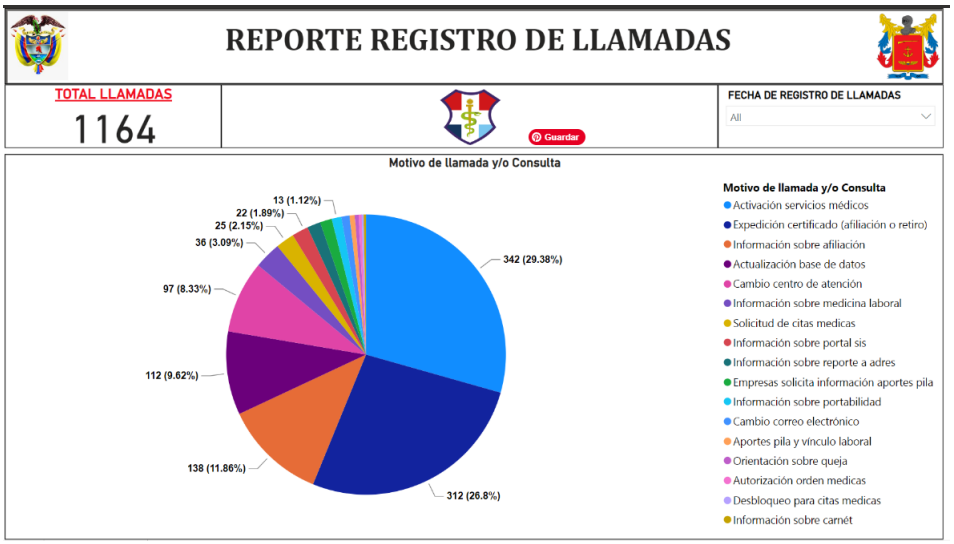


Ilustración *17.* Tablero Registro de llamadas

d. Tablero área de Afiliaciones

Este tablero permite visualizar las novedades en afiliación para todas las fuerzas, tomando como fuente de información SALUD.SIS

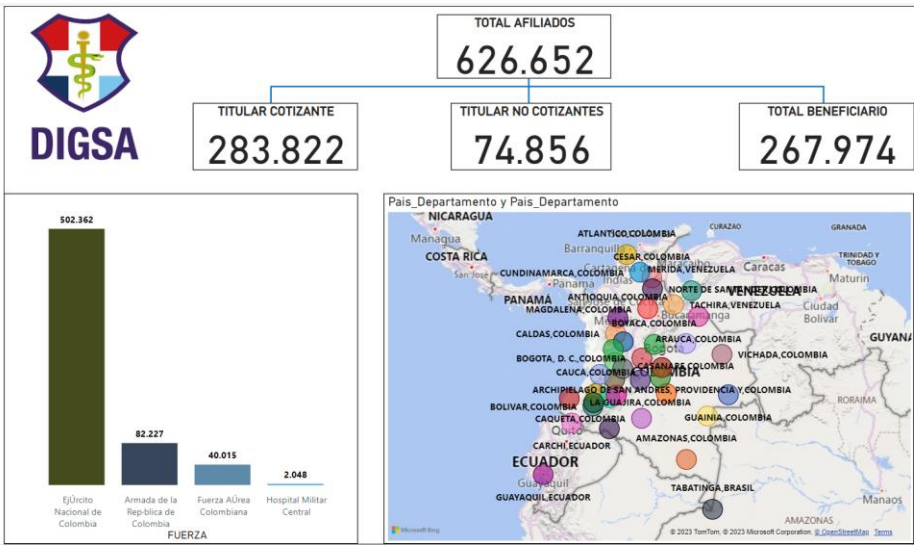


Ilustración *18.* Tablero Afiliaciones

e. Tablero área Jurídica

Este tablero permite visualizar el estado de los procesos jurídicos y PQR generados por los afiliados y sus familias.

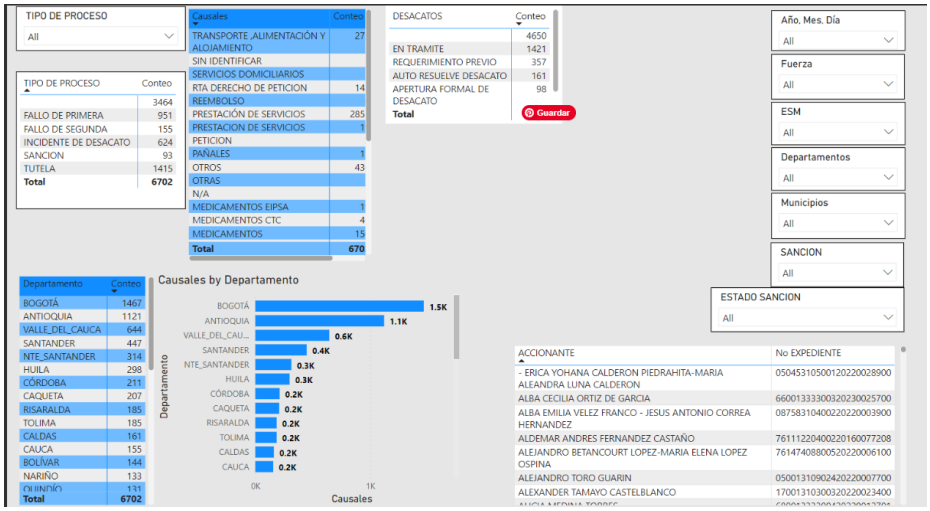


Ilustración 19. Tablero Jurídica

10.2.3. Gobierno de TI

Las TI en la entidad requieren disponer de un esquema / modelo administrativo de gobierno y gestión de las TIC que dé el direccionamiento y supervisión ejecutiva y además garantice el alineamiento, la planeación, organización, entrega de servicios de TI de manera oportuna, continua y segura.

El Gobierno de TI inicia con el análisis de la realidad organizacional de la entidad y con el contexto en el cual se desarrollará la Gestión de TI. Para este fin, se deben consultar los documentos que ya la entidad debe haber construido: la Arquitectura Institucional, el Marco Normativo, los Procesos de la Entidad, el Modelo de Gobierno y operación de la Entidad y los Mecanismos de contratación y compras públicas.

La Oficina de Tecnologías y Sistemas de Información, o quien haga sus veces, debe buscar la incorporación de Políticas de TI en la Organización, esto significa la expedición de documentos de Políticas de TI y su correspondiente divulgación a los diferentes grupos de interés.

10.2.4. Gestión de Sistemas de Información

Los sistemas de información y aplicaciones deben soportar los procesos de la DIGSA. Los lineamientos de este dominio permiten que la entidad diseñe, desarrolle, actualice, modifique o adquiera e implemente los sistemas de información que soporten de forma adecuada los procesos y procedimientos de la DIGSA, para ofrecer mejores trámites y servicios a los ciudadanos, entre otras obligaciones:

- Debe adoptar y personalizar una metodología alineada a las mejores prácticas para el desarrollo y mantenimiento de software, que oriente los proyectos de construcción o evolución de los sistemas de información que se desarrollen internamente o a través de terceros.
- Debe garantizar la construcción y gestión del catálogo de sistemas de información, el cual integra la caracterización de cada uno de sus sistemas de información. Las entidades cabeza de sector adicionalmente deben consolidar y mantener actualizado el catálogo de sistemas de información sectorial.
- Debe definir o adoptar una guía de estilo y usabilidad para la institución. Esta guía debe incorporar los lineamientos de gov.co y elementos de accesibilidad web.
- dentro de sus procesos, las actividades formales de análisis y gestión de requerimientos de software en el ciclo de vida de los sistemas de información de manera que se garantice su trazabilidad y cumplimiento.

Teniendo en cuenta las obligaciones, se continuará la implementación del modelo:

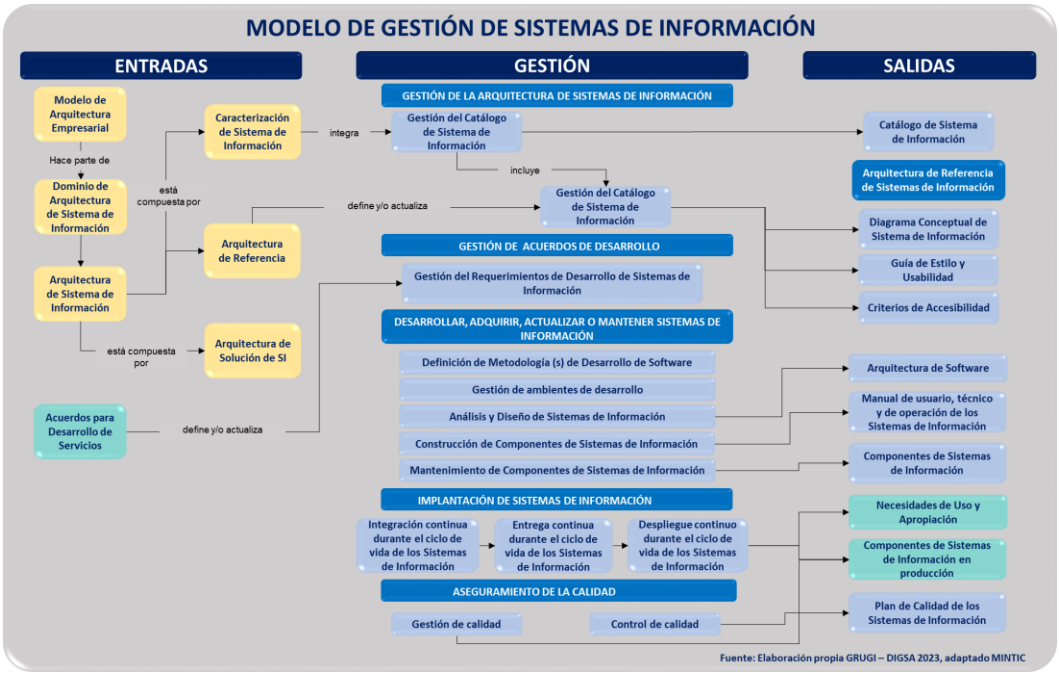


Ilustración *20.* Modelo de gestión de sistemas de información

10.2.5. Gestión de Servicios de TI

El Grupo Sistema Integral de Información Tecnologías de la Información y Comunicaciones (SISAM), deberá contar con un directorio actualizado de sus Servicios Tecnológicos, que le sirva de insumo para administrar, analizar y mejorar los activos de TI, debe gestionar la operación y el soporte de los servicios tecnológicos, en particular, durante la implementación y paso a producción de los servicios de TI, se debe garantizar la estabilidad de la operación de TI y responder acorde al plan de capacidad, entre otras obligaciones:

- Debe evaluar como primera opción la posibilidad de adquirir los Servicios Tecnológicos haciendo uso de la Nube (pública, privada o híbrida), para atender las necesidades de los grupos de interés.
- Debe garantizar la continuidad y disponibilidad de los servicios de TI, así como la capacidad de atención y resolución de incidentes para ofrecer continuidad de la operación y la prestación de todos los servicios de la entidad y de TI.
- Debe implementar capacidades de alta disponibilidad para las infraestructuras críticas y los Servicios Tecnológicos que afecten la continuidad del servicio de la institución, las cuales deben ser puestas a prueba periódicamente. debe velar por la prestación de los servicios de TI, identificando las capacidades actuales de los Servicios Tecnológicos y proyectando las capacidades futuras requeridas para un óptimo funcionamiento.
- Debe velar por el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos para los Servicios Tecnológicos. debe monitorear los recursos y servicios de TI y controlar el nivel de consumo de los recursos críticos que son compartidos por los Servicios Tecnológicos a fin de garantizar su disponibilidad.

Teniendo en cuenta las obligaciones del Grupo, se continuará la implementación del modelo:

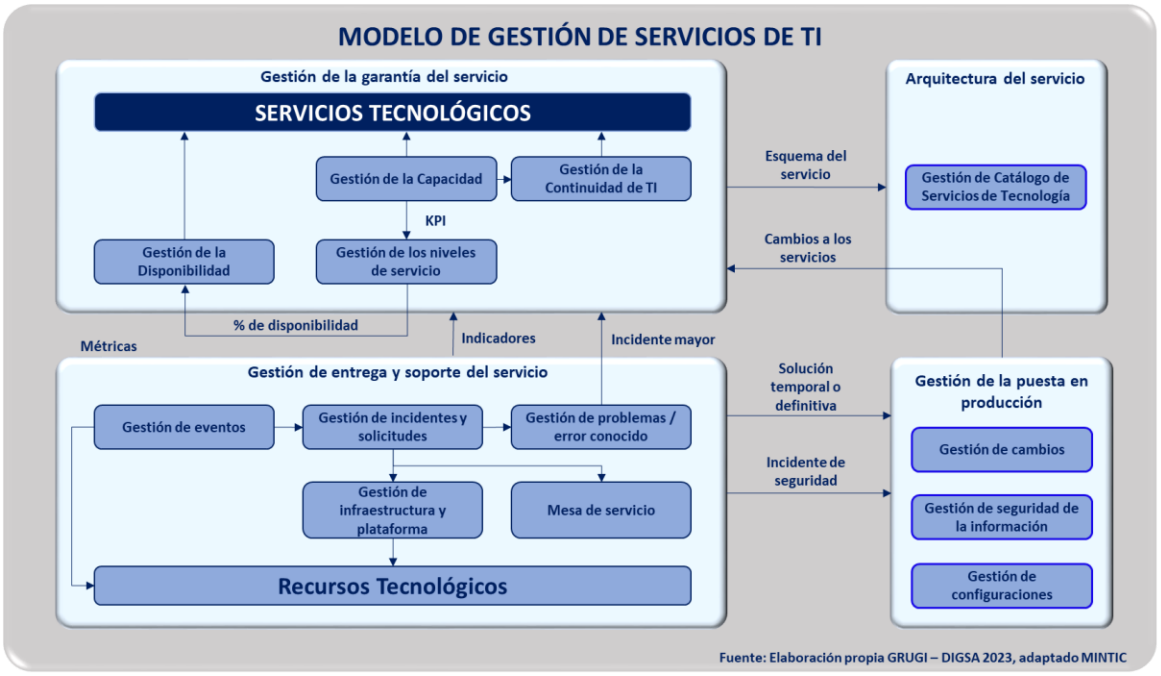


Ilustración *21.* Modelo Gestión de servicios TI

10.2.6. Estrategia de Comunicación y Socialización del PETI

El PETI como parte integral del modelo de gestión, establecerá una Estrategia de Comunicación y Socialización del PETI que se debe iniciar con la divulgación a nivel directivo, para después dar a conocer a las diferentes Áreas y Grupos de Trabajo de la entidad. Como parte del proceso de divulgación del PETI a continuación se indican las actividades que se deben incluir:

• Elaboración de presentación para reunión con los Coordinadores y Lideres de las Áreas y Grupos de Trabajo de la DIGSA.
• Elaboración de presentación para realizar con las Áreas y Grupos de Trabajo de la DIGSA.
• Publicación en el sitio web de la DIGSA.
• Publicación en la Intranet DIGSA.

Dentro de la Hoja de Ruta del PETI como: “Realizar divulgación y socialización PETI DIGSA 2023 - 2026 actualizado”, las actividades se ejecutarán para los periodos 2024 a 2026, teniendo en cuenta que la Estrategia, se debe elaborar después de recibir los documentos: Plan de Transformación Digital DIGSA y Diseño Política del Gobierno del Datos DIGSA, los cuales se entregarán a la DIGSA en diciembre del 2023. La mencionada Estrategia se elaborará con el acompañamiento del Área de Comunicaciones Estratégicas de la DIGSA (ARCOM).

10.2.7. Gestión de Seguridad

El Modelo de Seguridad y Privacidad de la Información - MSPI, impartirá lineamientos para la DIGSA en materia de actualización, implementación y adopción de buenas prácticas,

tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

El propósito es que la DIGSA, revise, actualice e incorpore la Seguridad de la Información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Sé encuentra revisara que este alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y la Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital y se actualizara mediante el Documento el Modelo de Seguridad y Privacidad de la Información y sus guías de orientación.

Ilustración *22.* Modelo seguridad y privacidad de la información

10.2.5.2 Sistema de Gestión de la Seguridad de la Información (SGSI)

El Sistema de Gestión de la Seguridad de la Información (SGSI), para la DIGSA, es un conjunto de políticas de administración de la información.

El concepto clave de un SGSI es el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando

asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Mediante la culminación de la implementación de la ISO/IEC 27001, se especificarán los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) en la DIGSA, mediante le modelo:

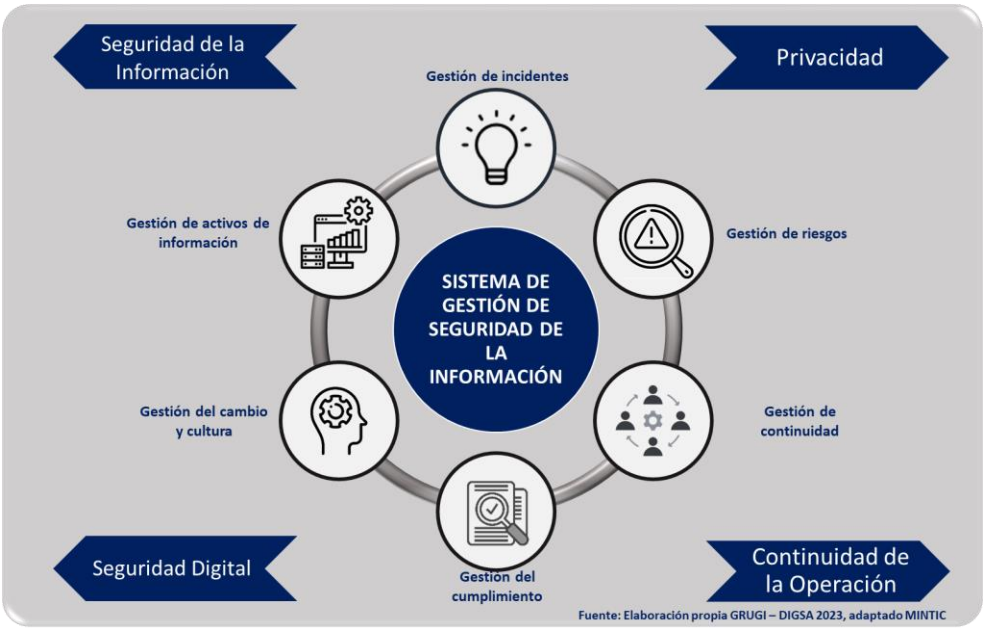


Ilustración *22.* Sistema de Gestión de Seguridad de la Información

10.2.8. Gestión de la Información

"La información es un asunto de todos", esta frase que debe ser un principio orientador de las arquitecturas de datos debería quedar en la mente de todos los funcionarios, y colaboradores de las entidades del Estado colombiano.

Todas las dependencias de la DIGSA deben estar involucradas con el Gobierno de la Información; no es responsabilidad exclusiva de los Grupos de trabajo de la Subdirección Técnica y de Gestión, Grupo Sistema Integral de Información Tecnologías de la Información y Comunicaciones (SISAM) y el Grupo de Gestión de la Información (GRUGI).

Existen diferentes modelos o arquetipos que permiten definir la estructura de Gobierno de la Información a nivel institucional, para la DIGSA e acuerdo a su con sus necesidades, se tomara como base el Modelo de Gestión de la I9nfromación que propone MINTIC, debe ser liderado por liderado por las áreas misionales o estratégicas de la entidad, apoyándose en los Grupos de Trabajo de la SUBTG:

Ilustración *23.* Modelo Gestión de la Información

10.2.9. Gestión de Uso y Apropiación de TI

Se realizará formulación de la Estrategia se Usó y Apropiación de TI para la Dirección General de Sanidad Militar, con la cual se buscará crear una cultura organizacional que permita adoptar el uso de herramientas tecnológicas a través de las políticas de TI y que los cambios que se generen para la mejora continua sean implementados de una manera proactiva, que genere valor y se refleje en los servicios que la entidad presta a los ciudadanos y a los grupos de valor. Este documento se desarrolla con base en las guías y lineamientos asociados al dominio de uso y apropiación del Marco de referencia de Arquitectura de TI y la Política de Gobierno Digital, buscando el posicionamiento de las tecnologías de información al interior de la DIGSA, buscando la modernización de sus procesos y procedimientos, lo que contribuirá a la transformación Digital, al uso y aprovechamiento de las Tecnologías, la consolidación de un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital, en el marco de la Política de Gobierno Digital que lidera de Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).

10.2.10. Proyecto SALUD.SIS

Los recursos provienen de inversión, obedecen a solucionar una necesidad de tipo estratégico que impacta a toda la organización, son nuevos proyectos que amplían las capacidades que se tienen actualmente. De igual manera el valor varía según el presupuesto asignado a la DIGSA y a la prioridad de los proyectos de inversión.

Análisis DOFA

ENTORNO INTERNO	
FORTALEZAS	**DEBILIDADES**
F1. Madurez del desarrollo y versatilidad de las funcionalidades con base en el modelo de atención en salud del SSFM.	D1. Falta de formación a stakeholders y product owner respecto a los procesos internos, la relación e integración de cada uno con las funcionalidades existentes y por desarrollar de SALUD.SIS.

F2. Infraestructura de avanzada para soportar la operación del sistema. F3. Soporte y ayuda 24/7 F4. Capacidad el sistema para ajustarse a los cambios normativos, de aplicaciones y base de datos. F5. Permite la modernización tecnológica para la reducción de costos y garantizar la seguridad a través del traslado del DATACENTER a la superficie FORTALEZA de Ministerio de Defensa. F6. Capacidad de adaptarse a los modelos de interoperabilidad estipulados por Ministerio de Salud. F7. Capacidad para el desarrollo de una única solución que unifique la ERP y la vertical en salud.	D2. Ausencia de formación de stakeholders y product owner en metodologías de proyectos y pedagogía en bases de datos y análisis de datos. D3. Constantes cambios en los estilos de liderazgo en cada nivel jerárquico. D4. Desconocimiento del modelo de salud, el marco normativo, sistemas de información y gestión de proyectos por parte de las directivas. D5. Imposibilidad de hacer interoperables los sistemas internos de información. D6. No contar con una única fuente (tercero) que realice las actualizaciones, desarrollos y procesos evolutivos del sistema de información SALUD.SIS D7. Incapacidad de suministrar a todos los ESM (independiente a su tamaño) infraestructura tecnológica (equipos de cómputo) y canal de conectividad (internet) con calidad y capacidad. D8. No garantizar la continuidad de los funcionarios por baja paga y crecimiento profesional e institucional. D9. Duplicidad en funcionalidad. D10. Malas prácticas en el diseño de las funcionalidades por partes del stakeholders
ENTORNO EXTERNO	
OPORTUNIDADES	**AMENAZAS**
O1. Potencializar SLAUD.SIS permitiría considerar certificar ESM para ofrecer y vender servicios en los territorios más alejados. O2. Capacidad para compartir información con los demás actores del sistema de salud en Colombia.	A1. Inferencia de desarrolladores o conglomerados de desarrollo para inferir en la toma de decisiones por parte de la dirección y los asesores. A2. Capacidad de EPS e IPS de implementar las actualizaciones de norma con ocasión de acceso rápido a los desarrollos de software. A3. Decisiones del orden ministerial que instruya dar por terminado el proyecto. A4. Evolución tecnológica a la cual no accede el SSFM. A5. Capacidad de las IPS y ARL para absorber la prestación de servicios asistenciales a los miembros activos, retirados, pensionados y sus beneficiarios de las FFMM con ocasión de ser más económico para el Estado y con mayor calidad y oportunidad.

Análisis DOFA

ANÁLISIS DOFA	OPORTUNIDADES	AMENAZAS

	O1. Potencializar SALUD.SIS permitiría considerar certificar ESM para ofrecer y vender servicios en los territorios más alejados**.** O2. Capacidad para compartir información con los demás actores del sistema de salud en Colombia**.**	A1. Inferencia de desarrolladores o conglomerados de desarrollo para inferir en la toma de decisiones por parte de la dirección y los asesores. A2. Capacidad de EPS e IPS de implementar las actualizaciones de norma con ocasión de acceso rápido a los desarrollos de software. A3. Decisiones del orden ministerial que instruya dar por terminado el proyecto. A4. Evolución tecnológica a la cual no accede el SSFM. A5. Capacidad de las IPS y ARL para absorber la prestación de servicios asistenciales a los miembros activos, retirados, pensionados y sus beneficiarios de las FFMM con ocasión de ser más económico para el Estado y con mayor calidad y oportunidad.
FORTALEZAS	**ESTRATEGIAS FO**	**ESTRATEGIAS FA**
F1. Madurez del desarrollo y versatilidad de las funcionalidades con base en el modelo de atención en salud del SSFM. F2. Infraestructura de avanzada para soportar la operación del sistema. F3. Soporte y ayuda 24/7 F4. Capacidad el sistema para ajustarse a los cambios normativos, de aplicaciones y base de datos. F5. Permite la modernización tecnológica para la reducción de costos y garantizar la seguridad a través del traslado del DATACENTER a la superficie FORTALEZA de Ministerio de Defensa. F6. Capacidad de adaptarse a los modelos de interoperabilidad estipulados por Ministerio de Salud.	F1-F2-F4-F5-O1: Solicitar a través del Ministerio de Defensa la prioridad de fortalecer el rol del Estado como garante del acceso a internet para todos, generando incentivos y facilidades para la inversión en infraestructura en las zonas alejadas o con baja conectividad. F3-F6-F7-O2: Presentar al Gobierno Nacional la solicitud de priorizar la inversión nacional en salud digital, con el fin de consolidar una infraestructura que permita la interconexión e interoperabilidad de las bases de datos y aplicaciones de todo el sector salud, a fin de facilitar el acceso a los datos en el momento oportuno.	F1-F2-F6-F7-A1-A4: Fortalecer el desarrollo e infraestructura tecnológica para lograr la compatibilidad con la nueva tecnología. F4-A3: Adaptar y ajustar los procesos y procedimientos que permitan la inclusión de la operación administrativa y operativa del sistema en las diferentes actividades que impacta en la Entidad. F5-A2-A5: Aprovechar los servicios y sistemas tecnológicos de avanzada que provee el Ministerio de Defensa con el fin de reducir la brecha en la capacidad de implementación de las nuevas tecnologías en comparación con los otros actores del sistema de salud en Colombia.

F7. Capacidad para el desarrollo de una única solución que unifique la ERP y la vertical en salud.		
DEBILIDADES	**ESTRATEGIA DO**	**ESTRATEGIA DA**
D1. Falta de formación a stakeholders y product owner respecto a los procesos internos, la relación e integración de cada uno con las funcionalidades existentes y por desarrollar de SALUD.SIS. D2. Ausencia de formación de stakeholders y product owner en metodologías de proyectos y pedagogía en bases de datos y análisis de datos. D3. Constantes cambios en los estilos de liderazgo en cada nivel jerárquico. D4. Desconocimiento del modelo de salud, el marco normativo, sistemas de información y gestión de proyectos por parte delas directivas. D5. Imposibilidad de hacer interoperables los sistemas internos de información. D6. No contar con una única fuente (tercero) que realice las actualizaciones, desarrollos y procesos evolutivos del sistema de información SALUD.SIS D7. Incapacidad de suministrar a todos los ESM (independiente a su tamaño) infraestructura tecnológica (equipos de cómputo) y canal de conectividad (internet) con calidad y capacidad. D8. No garantizar la continuidad de los funcionarios por baja paga y crecimiento profesional e institucional. D9. Duplicidad en funcionalidad. D10. Malas prácticas en el diseño de las funcionalidades por partes del stakeholders	D1-D2-D3-D4-D8-D10-O1: Crear un plan de capacitación enfocando el objetivo en el uso y manejo de las funcionalidades de SALUD.SIS para fortalecer las actividades de inducción y reinducción y posterior, realizar una gestión del conocimiento exitosa. D5-D6-D7-D9-O2: Plantear de manera conjunta (Estado – SSFM - Otras entidades) se adquieran bienes de salud pública con el uso de un software de intercambio e interoperabilidad para la toma de decisiones automática, entre otras funcionalidades.	D1-D2-D3-D4-D10-A1: Establecer un lineamiento que delimite el rol de los desarrolladores y asesores en la entidad, con el propósito de enfocar ciertos roles y responsabilidades en las personas que intervienen en los procesos internos de los sistemas de información. D5-D6-D7-D9-A2-A3-A4: Solicitar las bases de datos e información en general que servirían para construir un software propio con funcionalidades similares a SALUD.SIS.

Tabla 22. Gestión y Supervisión del Presupuesto de Inversiones y Gastos de Operación

OBJETIVO	PRODUCTO	META	ACTIVIDAD	VALOR ACTIVIDAD 2023	VALOR ACTIVIDAD 2024	VALOR ACTIVIDAD 2025	VALOR ACTIVIDAD 2026
Desarrollar herramientas para la planeación, control y seguimiento de los recursos	Servicios de información actualizados		Desarrollar la ERP y las funcionalidades finales de la Vertical en Salud	3.500.000.000	3.200.000.000	2.700.000.000	1.700.000.000
			Implementar SALUD.SIS	180.000.000	180.000.000	180.000.000	180.000.000
			Gestionar el Cambio	0	0	0	0
Implementar procesos que garanticen la ejecución de actividades en la Prestación de Servicios de Salud (incluye estrategia de Atención Primaria en Salud (APS) y el Modelo Integral de Atención en Salud (MAIS))	Servicios tecnológicos	95	Gestionar la adquisición del servicio de DATACENTER para el desarrollo e implementación del sistema de información a nivel nacional	2.166.000.000	1.100.000.000	1.200.000.000	1.200.000.000
			Gestionar la adquisición del Hardware para la implementación del sistema de información a nivel nacional	2.403.000.000	0	0	0
			Dotar Redes y comunicaciones para el Sistema	3.685.000.000	780.000.000	0	0
			Realizar soporte técnico (Mantenimiento software, mesa de servicio)	2.692.000.000	2.826.000.000	2.967.000.000	3.115.000.000
			Gestionar la adquisición del Mantenimiento Licencias ERP	0	0	0	0
			Prestar servicios Administrativos	130.000.000	130.000.000	130.000.000	130.000.000
			Realizar Mantenimiento Técnico Equipos TI	98.000.000	98.000.000	98.000.000	98.000.000
			TOTALES	14.854.000.000	8.314.000.000	7.275.000.000	6.423.000.000

Fuente: Información propia SISAM

10.2.11. Estructura y Organización humana de TI

Teniendo en cuenta el plan de desarrollo del actual gobierno, el SSFM desde su Subdirección Técnica y de Gestión, específicamente desde la gerencia el proyecto SALUD.SIS, construye las políticas para la modernización de las tecnologías de la información.

La estructura de la jefatura de tecnologías de la información deberá quedar de la siguiente forma:

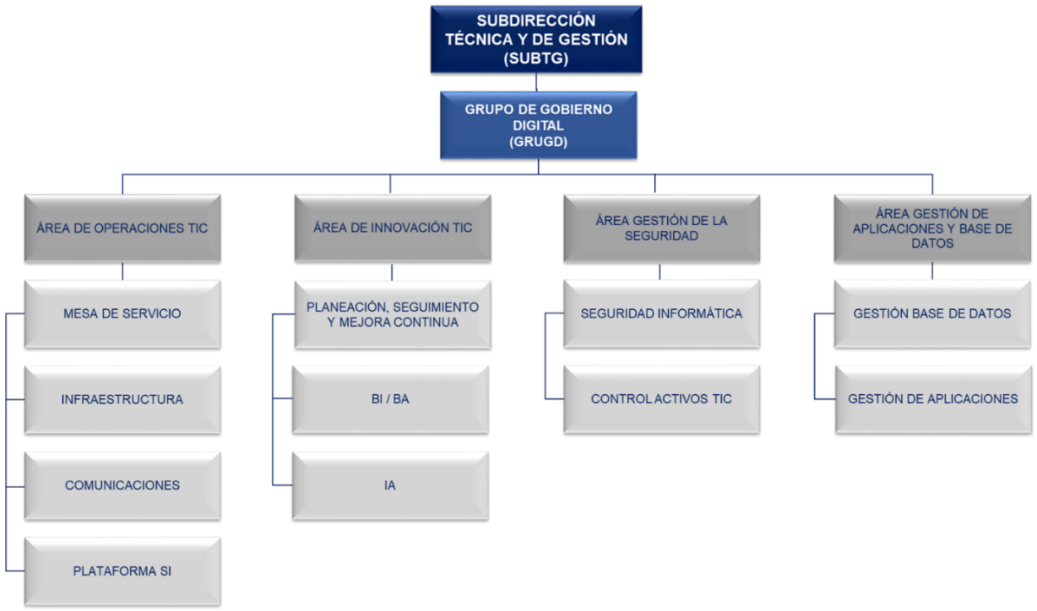


Ilustración 11. Estructura y Organización humana de TI

Para poder cumplir con el objetivo estratégico se hace necesaria esta estructura teniendo en cuenta que el personal debe contar con el perfil y competencia idónea.

10.2.12. Gestión de proyectos

- Todos los proyectos de tecnología de la información y comunicaciones son viabilizados inicialmente por el Comité de integración de tecnologías de Información (CITI), utilizando la metodología que cuenta para este propósito.

- Cuando son proyectos de inversión estos son inscritos en el Banco de Programas y Proyectos (BPIN) del Departamento Nacional de Planeación (DNP) bajo la metodología MGA y luego son viabilizados año a año en los Comités Funcionales.

- Para todos los procesos de contratación se define de manera integral y completa las actividades necesarias para evaluar los aspectos legales asociados a un proyecto, desde su estructuración, estudio de viabilidad, contratación y cierre.

10.3. Gestión de Información

Como se hizo referencia la entidad cuenta con varias fuentes de información que no se cuentan integradas entre sí, uno de los objetivos es unificar la Arquitectura de la Información mediante un modelo por capas proporciona un grupo de servicios independiente, y estos se integran unos con otros para proporcionar todas las funciones de la plataforma. Estos pilares se pueden describir de la manera siguiente:

- Capa de gobernanza: la implementación de esta capa almacena y mantiene la seguridad, la gobernanza de datos y las políticas del ciclo de vida de los datos que aplican los componentes de la capa de la plataforma. Incluye los procesos y políticas que permiten

mantener el orden en la plataforma de datos y garantizar que los metadatos nos permitan implementar las prioridades del negocio.

- Capa de infraestructura: servicios de uso y gestión de la plataforma necesarios para el funcionamiento continuo de la arquitectura. Esto incluye servicios de DevOps para permitir la gestión permanente de entregas, clústeres y recursos, así como el abastecimiento de la nube, entre otros.
- Capa de la plataforma: una combinación de productos y componentes que proporciona los servicios básicos para el alojamiento y ejecución de aplicaciones, facilitando el trabajo en tareas como el acceso a datos, manipulación de los datos, ejecución de lógica de negocio, etc.
- Capa de consumo de datos: cualquier conjunto de datos de clientes externos e internos relevante para los usuarios se puede cargar a la plataforma mediante la capa de ingestión, de una manera configurable y automatizada.
- Capa de aplicaciones: ubicación para todas las actividades específicas de las aplicaciones de la empresa que admite la plataforma. Se espera que estas consten de procesamiento y cálculo de datos que precisen gran cantidad de recursos adecuados a las soluciones de la plataforma de datos de la empresa. Además de esto, también podría requerirse una sofisticada gestión, organización y orquestación de los recursos.
- Capa de interacción de usuarios: proporciona funciones de interacción para el usuario, como análisis, búsquedas, minería de datos, informes estándar, etc.

A la fecha la entidad cuenta con varias fuentes de información que no se cuentan integradas entre sí, generando inconvenientes a la hora de tomar decisiones por no contar con información unificada.

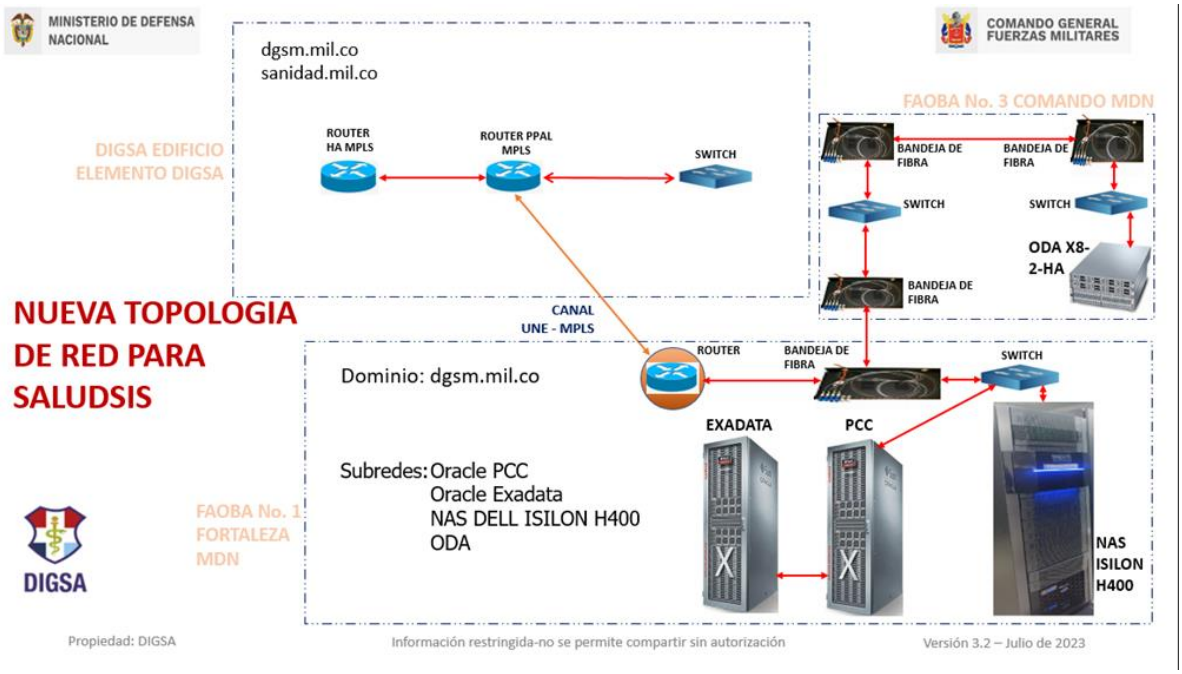


Ilustración 12. Modelo de Gestión de la Información -Fuente SISAM

10.3.1. Gestión de la calidad y seguridad de la información

Actualmente se tienen sistemas de información que están desarrollados en diferentes herramientas y no cuentan con ambientes de desarrollo y calidad que permitan realizar el control de cambios sin afectar el ambiente productivo.

Así mismo la información almacenada en las bases de datos de los sistemas de información no cuentan con un alto nivel de calidad, para lo cual se proyecta implementar la analítica de datos que coadyuve al modelamiento de resultados asistenciales, mejoramiento en las decisiones y desarrollo de proyecciones.

10.3.2. Análisis y Aprovechamiento de los Componentes de información

Se está construyendo una herramienta de inteligencia de negocios que sirve de análisis para cada uno de los componentes de información con que se cuenta a través de los flujos de información de cada uno de los procesos de la entidad.

10.3.3. Desarrollo de capacidades para el uso de la información

La DIGSA mantendrá la administración de datos maestros en alineación con el Sistema Integral de Información SALUD.SIS, cualquier proyecto que emprenda el Subsistema de Salud de las Fuerzas Militares en materia de Sistemas de información institucional debe estar alineado con esta política y sus lineamientos derivados, por lo tanto, es deber de los interesados gestionar la comunicación con las áreas directamente encargadas de esta política basados en este documento.
Teniendo en cuenta el ámbito del dato se debe tener presente lo siguiente:

- El dato generado por la DIGSA es de índole público: El intercambio de datos abiertos e interoperabilidad permitirá dar cumplimiento al dato generado por medio de: Acceso a los Datos, Ley de Transparencia, Apertura de Datos e Interoperabilidad de Datos, siguiendo las políticas de confidencialidad teniendo en cuenta que es información sensible.

  Por lo tanto, la DIGSA buscará publicar su información pública en el portal de datos abiertos del estado, esta actividad estará coordinada y es responsabilidad del Área de Comunicaciones Estratégicas y Gestión del Cambio.

- Los datos se producen bajo atributos de calidad: Todos los datos e información que produzca la DIGSA se realizarán bajo procesos que respondan con los atributos de calidad de la administración de datos maestros, ciclo de vida de los datos, mapa de información, migración y procesos de calidad de la información.

Como resultado de la gestión de la información se obtienen mecanismos de usos y accesos disponibles, información de calidad, generación de valor a partir de la información, apoyo a la toma de decisiones e instrumentos de análisis de la información disponible para los usuarios de la Dirección General de Sanidad Militar (DIGSA).

10.4. Sistemas de Información

Como su nombre lo indica, va dirigido en primera instancia a los desarrolladores de software para que puedan comprender técnicamente, pero de manera simple, cuál es la arquitectura de software ideada para el Sistema de Información de Salud de las Fuerzas Militares. Esto se aprecia en el siguiente diagrama de aplicaciones, el cual abarca todas las decisiones y opciones que se tendrían para desarrollar cualquier módulo funcional en cualquiera de las fases de la solución de la vertical de salud, ya que expone de manera genérica los modelos aplicados.

Desde el Cliente se consume la aplicación web del servidor, es la primera parte de la distribución cliente-servidor. El cliente puede ser un navegador web o algún sistema externo a la aplicación de la vertical de salud. En el caso de un navegador web, se pueden manejar dos estilos de interfaces gráficas, MVC y SPA.

En el estilo o patrón MVC, un usuario de la aplicación navega a través de ella siguiendo un flujo de trabajo paso a paso que lo lleva de una vista (página web en HTML) a otra, lo que implica cargar nuevas vistas o recargarlas. En el caso de SPA, las vistas o páginas normalmente permanecen activas por más tiempo y son mucho más interactivas, por lo que resultan ideales para implementar paneles de control y casos de uso similares.

10.4.1. Catálogo de los Sistemas de información

El dominio de Sistemas de Información propone que para soportar los procesos de direccionamiento estratégico, misionales y de apoyo en una organización, es importante contar con sistemas de información que se conviertan en fuente única de datos útiles para la toma de decisiones en todos los aspectos; que garanticen la calidad de la información, dispongan recursos de consulta a los públicos de interés, permitan la generación de transacciones desde los procesos que generan la información y que sean fáciles de mantener. Que sean escalables, interoperables, seguros, funcionales y sostenibles, tanto en lo financiero como en la parte técnica, el catálogo de los sistemas de información es el siguiente:

Tabla 23. Catálogo de los Sistemas de información software interno

Software	Plataforma	Compatible con IPv6
Kactus	Delphi	SI
ERP	SAP	SI
Vertical de salud SALUD.SIS	VISUAL.NET	SI
Sistema de gesti6n documental ONBASE	Sin información	NO

Página WEB (Micrositios)	PHP	SI
Correspondencia	Access 2010	SI
Profesionales en salud	PHP	SI

Fuente: Información propia SISAM

Software externo con el que se interactúa

Tabla 24. Software externo interactúan IPv6

Software	Plataforma	Compatible con IPv6
Siif nación	Visual.net	NA
Suite Visión	JSP	NA
Antivirus (kaspersky	Windows	NA
Correo electrónico (outlook)	Windows	NA
Mesa de ayuda (msl)	Sin información	NA
Plataforma seguridad (palo alto)	Sin información	NA

Fuente: Información propia SISAM

10.4.2. Arquitectura de Referencia

En el estado actual de la DIGSA se ha adoptado una arquitectura de referencia, para ecosistemas de aplicaciones complejos, como el proceso estructural de SALUD.SIS el cual adopta una estandarización de las decisiones de diseño de la siguiente manera:

Ilustración 13. Arquitectura de Referencia

Dentro de la estandarización de decisiones de diseño para la DIGSA, se puede contemplar:

- Componentes transversales de seguridad que ayudan a auditar las acciones en los sistemas, el componente de seguridad es una solución transversal de log de transacciones.

10.4.3. Mantenimiento de los Sistemas de información

Tabla 25. Mantenimiento de los Sistemas de Información

Actividad	Grado de madurez	Descripción hallazgo u oportunidad de mejora
Mantenimientos Preventivos	Implementado	Este mantenimiento está orientado a revisar, monitorear, estudiar y proponer soluciones a incidencias o inexactitudes en el sistema, basándose en la información recabada a partir de las tareas de análisis, revisión y monitoreo, se revisarán: - Errores descubiertos en SOFTWARE en productivo - Diagnostico a los errores descubiertos - Posible resolución de errores descubiertos

Actividad	Grado de madurez	Descripción hallazgo u oportunidad de mejora
Mantenimientos Evolutivo	Implementado	Orientado al análisis, diseño, desarrollo y entrega de soluciones nuevas y necesarias para cubrir las actualizaciones o nuevas funcionalidades de los módulos en productivo del sistema. El mantenimiento evolutivo se elaborará así: - Descripción requerimientos escalada al proveedor del servicio - Tiempo de resolución de los requerimientos escalados al proveedor - Descripción requerimientos solucionados - Descripción requerimientos rechazados - Relación de tiempo descontado de la bolsa por requerimiento - porcentaje de avance por cada solución en desarrollo
Mantenimientos Correctivos	Implementado	En caso de mal funcionamiento, el proveedor efectuara mantenimiento correctivo, reingeniería de las funcionalidades, web service y/o componentes de software donde se presenten incidentes, fallas o errores, se revisarán: - El proveedor realizara diagnóstico del incidente o falla escalado por el comité de cambios de DIGSA - Hacer análisis de la solución y entregar el formato de control de cambios - Hacer el diseño y desarrollo de la solución - Hacer pruebas de la solución en el entorno de pruebas, incluyendo pruebas unitarias e integrales debidamente documentadas y en coordinación con el comité de control de cambios

Fuente: Información propia SISAM

10.4.4. Soporte de los Sistemas de Información

Tabla 26. Soporte de los Sistemas de Información

Prioridad	Tiempo de respuesta	Descripciones de los niveles de servicios
1	2 horas (en horario 7*24)	"Caída del sistema" o situación del producto inoperativo que afecta al entorno de producción y la conectividad de la institución.
2	4 horas (en horario 7*24)	Situación con repercusiones importantes para el negocio que probablemente pone en peligro el entorno de producción. El o los Switches pueden funcionar, pero de forma muy limitada.
3	6 horas (en horario 7*24)	Situación con repercusiones poco importantes para el negocio con la mayoría de las funciones del o los Switches están en funcionamiento. Sin embargo, puede ser necesaria algún tipo de estrategia para poder restaurar el servicio.
4	24 horas (en horario 7*24)	Problema o cuestión menor que no afecta al funcionamiento de la plataforma.

Fuente: Información propia SISAM

10.5. Infraestructura TI

La DIGSA cuenta con un DataCenter donde se encuentra la plataforma tecnológica que soporta los sistemas de información administrativos y los servicios TIC, el cual cuenta con las condiciones mínimas de operación, para garantizar el acceso y la disponibilidad.

En la actualidad se cuenta con equipos de hiperconvergencia para manejar la administración de la infraestructura de TIC, a la fecha se han tenido entre otros los siguientes beneficios:

Eficiencia de datos, movilidad, Escalabilidad y eficiencia, protección de datos, alta disponibilidad, eficiencia de costos, centralización de máquinas virtuales, simplificación del Data Center y reducción de costos de TCO (Costo Total de Propiedad).

10.5.1. Arquitectura de Infraestructura tecnológica

La administración de la capacidad de la infraestructura tecnológica para la DIGSA, las cuales definen elementos claves a gestionar:

- Infraestructura (Centro de Computo – Nube)
- Hardware y Software de Oficina
- Conectividad
- Red Local e Inalámbrica
- Red WAN
- IPV6
- Gestión de ANS

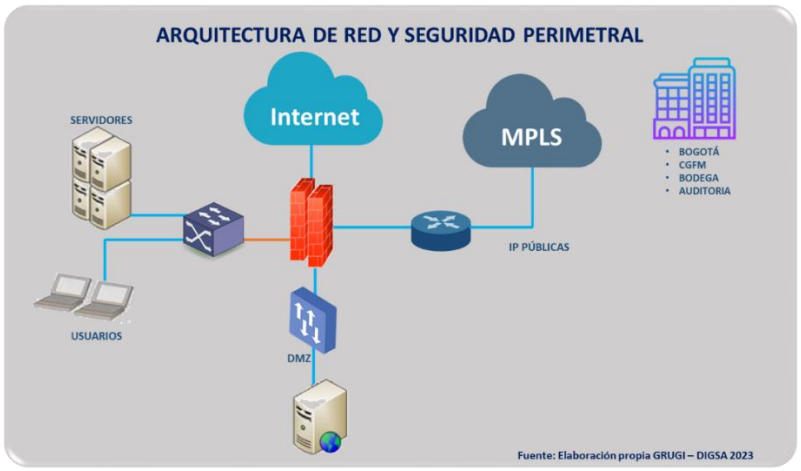


Ilustración 14. Arquitectura de Infraestructura tecnológica

10.5.2. Gestión Operativa de Servicios Tecnológicos

La Gestión Operativa de tecnológicos la entidad busca garantizar la disponibilidad y continuidad de los servicios tecnológicos por medio de procesos, procedimientos, actividades y herramientas.

11. PORTAFOLIO DE INICIATIVAS, PROYECTOS Y MAPAS DE RUTA

11.1. Plan de Acción - Conformación de Iniciativas y Proyectos

PROYECTO	DESCRIPCIÓN	INVERSIÓN	
Formulación diseño e implementación del Sistema de información para el Subsistema de Salud de las Fuerzas Militares a nivel nacional, Código BPIN: 2018011000614	Desarrollo de funcionalidades del Software de la Vertical de salud e interoperabilidad	$ 11.100.000.000,00	$ 35.954.000.000,00
	Implementar SALUD.SIS	$ 720.000.000,00	
	Dotar Redes y comunicaciones para el Sistema	$ 4.465.000.000,00	
	Gestionar la adquisición del Hardware para la implementación del sistema de información a nivel nacional.	$ 2.403.000.000,00	
	Gestionar la adquisición del servicio de DATACENTER para el desarrollo e implementación del sistema de información a nivel nacional	$ 5.666.000.000,00	
	Servicio de soporte y mantenimiento.	$ 11.600.000.000,00	

Tabla 27. Iniciativas y Proyectos

11.2 Acciones - Hoja de Ruta

HOJA DE RUTA PETI DIGSA 2023 - 2026								
Acción: Implementar los mecanismos de seguimiento y control frente al cumplimiento de las Políticas y Lineamientos emitidos por el CSSMP para el SSFM								
Producto	**Actividad SSFM**	**Descripción de la actividad DIGSA**	**Producto - Periodicidad**	**Presupuesto**				**Indicador**
				2023	**2024**	**2025**	**2026**	
Documento PETI DIGSA 2023 - 2026	Actualizar y elaborar el documento PETI DIGSA 2023 - 2026	Se actualiza y elabora documento PETI, según lineamientos y metodología de MINTIC, MDN y Planeación Estratégica DIGSA.	Anual	0	0	0	0	Documento PETI 2023 - 2026

Soporte de remisión del PETI DIGSA 2023 - 2026 para revisión	Remitir PETI DIGSA 2023 - 2026 a Grupo de Planeación Estratégica DIGSA para revisión	Se remite el documento PETI 2023 - 2026 DIGSA, para revisión y aprobación del Grupo de Planeación Estratégica de la DIGSA, para posterior aprobación del Comité Institucional de Gestión y Desempeño	Anual	0	0	0	0	Soporte remisión
Soporte de presentación y aprobación del PETI DIGSA 2023 - 2026 a Comité Institucional de Gestión y Desempeño	Presentación PETI DIGSA 2023 - 2026 a Comité Institucional de Gestión y Desempeño	Se presenta PETI 2023 - 2026 DIGSA por parte del GRUGI	Anual	0	0	0	0	Acta aprobación
Documento Plan de Transformación Digital DIGSA y anexos	Elaborar documento Plan de Transformación Digital DIGSA	Ejecutar el contrato Electrónico No. 168 DIGSA-2023	Anual	150.000.000	0	0	0	Documento Plan de Transformación Digital DIGSA y anexos
Documento Diseño Política del Gobierno del Datos DIGSA y anexos	Elaborar documento Diseño Política Gobierno de Datos DIGSA	Ejecutar el contrato Electrónico No. 144-DIGSA-2023	Anual	27.187.200	0	0	0	Documento Política Gobierno de Datos DIGSA y anexos
Hoja de ruta para el despliegue del Plan de Transformación Digital DIGSA 2024 - 2026	Elaborar hoja de ruta para el despliegue del Plan de Transformación Digital DIGSA 2024 - 2026	A partir del documento del Plan de Transformación Digital, ajustar las actividades del PETI 2023 - 2026 y actualizar la hoja de ruta	Anual	0	0	0	0	Hoja de ruta para el despliegue del Plan de Transformación Digital DIGSA 2024 - 2026
Hoja de ruta para el despliegue del Diseño del Gobierno del Datos DIGSA 2024 - 2026	Elaborar hoja de ruta para el despliegue del Diseño del Gobierno del Datos DIGSA 2024 - 2026	A partir del documento del Diseño de Política del Gobierno de Datos, ajustar las actividades del PETI 2023 - 2026 y actualizar la hoja de ruta	Anual	0	0	0	0	Hoja de ruta para el despliegue del Diseño del Gobierno del Datos DIGSA 2024 - 2026

Documento PETI DIGSA 2023 - 2026 actualizado	Actualizar el PETI DIGSA 2023 - 2026.	Actualizar el PETI DIGSA 2023 - 2026, según hojas de ruta del Diseño del Gobierno del Datos DIGSA y del Plan de Transformación Digital DIGSA	Anual	0	0	0	0	Documento PETI 2023 - 2026
Soporte de remisión del PETI DIGSA 2023 - 2026 actualizado, para revisión	Remitir PETI DIGSA 2023 - 2026 a Grupo de Planeación Estratégica DIGSA para revisión	Remitir el documento PETI 2023 - 2026 DIGSA actualizado, para revisión y aprobación del Grupo de Planeación Estratégica de la DIGSA	Anual	0	0	0	0	Soporte remisión
Soporte de presentación y aprobación del PETI DIGSA 2023 - 2026 actualizado, a Comité Institucional de Gestión y Desempeño	Presentación PETI DIGSA 2023 - 2026 a Comité Institucional de Gestión y Desempeño	Se presenta PETI 2023 - 2026 DIGSA actualizado, por parte del GRUGI	Anual	0	0	0	0	Acta aprobación
Actas divulgación y socialización PETI DIGSA 2023 - 2026 actualizado	Realizar divulgación y socialización PETI DIGSA 2023 - 2026 actualizado	Se realiza divulgación y socialización del PETI 2023 - 2026 DIGSA actualizado	Anual	0	0	0	0	Actas Capacitación

11.3 Proyección de inversión en funcionamiento TI

PROYECCION GASTOS FUNCIONAMIENTO - SISAM (MILES DE MILLONES)						
id	**Task Name**	**Responsable**	**AÑO 1**	**AÑO 2**	**AÑO 3**	**AÑO 4**
1	Computadores de mesa	TC Elizabeth Bocarejo	$ 1.790.000	$ 1.795.370	$ 1.800.756	$ 1.806.158
2	Repuestos (discos duros de estado sólido)	TC Elizabeth Bocarejo	$ 6.250	$ 6.269	$ 6.288	$ 6.306
3	Repuestos (Memorias RAM DDR4 8GB)	TC Elizabeth Bocarejo	$ 4.625	$ 4.639	$ 4.653	$ 4.667
4	Licenciamiento Office 365 para servicios en la nube por un año + Devops	TC Elizabeth Bocarejo	$ 600.400	$ 602.201	$ 604.008	$ 605.820
5	Licenciamiento end point seguridad	TC Elizabeth Bocarejo	$ 202.500	$ 203.108	$ 203.717	$ 204.328
6	Licenciamiento soporte firewall palo alto por un año	TC Elizabeth Bocarejo	$ 300.000	$ 300.900	$ 301.803	$ 302.708
7	comunicaciones estratégicas - licenciamiento de suite adobe acrobat pro- licencia adobe stock	TC Elizabeth Bocarejo	$ 15.000	$ 15.045	$ 15.090	$ 15.135
8	solución en seguridad de correo electrónico FORTIMAIL	TC Elizabeth Bocarejo	$ 80.000	$ 80.240	$ 80.481	$ 80.722
9	Mantenimiento Licencias SAP	TC Elizabeth Bocarejo	$ 2.120.000	$ 2.126.360	$ 2.132.739	$ 2.139.138
10	Licenciamiento Monitoreo de red e infraestructura	TC Elizabeth Bocarejo	$ 200.000	$ 200.600	$ 201.202	$ 201.805
11	Servicio SOC, NOC, SOAR,SASE Para seguridad, monitoreo, protección y gestión de seguridad.	TC Elizabeth Bocarejo	$ 300.000	$ 300.900	$ 301.803	$ 302.708
12	Licenciamiento OnBase	TC Elizabeth Bocarejo	$ 180.000	$ 180.540	$ 181.082	$ 181.625
13	Licenciamiento, soporte y mantenimiento -Kactus - modulo Smart people	TC Elizabeth Bocarejo	$ 70.000	$ 70.210	$ 70.421	$ 70.632
14	Transformación Digital en salud	TC Elizabeth Bocarejo	$ 500.000	$ 501.500	$ 503.005	$ 504.514
15	Pagina web-hosting	TC Elizabeth Bocarejo	$ 600.000	$ 601.800	$ 603.605	$ 605.416
16	Continuidad del negocio - servicio en la nube	TC Elizabeth Bocarejo	$ 100.000	$ 100.300	$ 100.601	$ 100.903
17	Canales dedicados y conexión a internet- fortaleza	TC Elizabeth Bocarejo	$ 150.000	$ 150.450	$ 150.901	$ 151.354
18	Switches Access point	TC Elizabeth Bocarejo	$ 1.200.000	$ 1.203.600	$ 1.207.211	$ 1.210.832

19	Servicios de mantenimiento, soporte y mantenimiento preventivo y correctivo	TC Elizabeth Bocarejo	$ 400.000	$ 401.200	$ 402.404	$ 403.611
20	Servicio de conmutador telefonía C3	TC Elizabeth Bocarejo	$ 200.000	$ 200.600	$ 201.202	$ 201.805
21	Licenciamiento Software Backus	TC Elizabeth Bocarejo	$ 200.000	$ 200.600	$ 201.202	$ 201.805
22	Extensión de garantía de servidores	TC Elizabeth Bocarejo	$ 300.000	$ 300.900	$ 301.803	$ 302.708
23	Adquisición de servicios profesionales para la implementación del modelo de soporte nivel II, redes e infraestructura	TC Elizabeth Bocarejo	$ 400.000	$ 401.200	$ 402.404	$ 403.611

11.4 Cronograma de funcionamiento TI

12. BIBLIOGRAFÍA

- Documento - versión actualizada del modelo de gestión TI
- Plan Estratégico de Tecnologías de Información (PETI) de MinTIC 2019 – 2023, https://www.mintic.gov.co/portal/604/articles-5271_Peti.pdf.
- Plan Estratégico de Tecnologías de la Información y las Comunicaciones del Sector Defensa y Seguridad 2018 – 2022
- Guía Para la formulación y seguimiento de planes institucionales (Junio 2021)

LISTA DE ILUSTRACIONES

LISTA DE TABLAS