DIRECCIÓN GENERAL
DE SANIDAD MILITAR

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES PETI 2023-2026

2025

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
4	Noviembre 2024	Se ajustó el documento, por actualización de guía para la formulación y seguimiento de planes institucionales MDN-COGFM-PROPLAES-DIGSA-GI.95.1-3. Vigencia 2023 EL documento es aprobado mediante el Acta 0123013530002MDN-COGFM-JEMCO-DIGSA-GRUPL-ARDEI-29.75 del 05 de diciembre 2023, por el Comité Institucional de Gestión y Desempeño, para esta versión se actualiza bajo los parámetros MINTIC Plan Estratégico de Tecnologías de Información (PETI) de MinTIC 2022 versión 3 y guía y la plantilla tipo cartilla PETI plus y MRAE 2023 de MINTIC 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
5	Diciembre 2024	Se ajustó el documento, por actualización de guía para la formulación y seguimiento de planes institucionales MDN-COGFM-PROPLAES-DIGSA-GI.95.1-3. Vigencia 2025 El documento es aprobado mediante el Acta 0124014834002/MDN-COGFM-JEMCO-DIGSA-GRUPL-ARDEI-2.25 del 27 de diciembre 2024, por el Comité Institucional de Gestión y Desempeño de la Dirección General de Sanidad Militar, se actualiza versión por ajustes en nombre del plan en el pie de página y otros requerimientos MDN-COGFM-PROPLAES-DIGSA-GI.95.1-3. Vigencia 2025 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

Aprobó:	Comité de Gestión y Desempeño Institucional Dirección General de Sanidad Militar Acta N° 0124014834002 de 2024	
Revisó:	CR. Alexander Peña Cristancho Subdirector Técnico y de Gestión DIGSA	TC. Jorge Darwin Guevar Coordinadora Grupo Sistema Integral de Tecnologías de la Información y Comunicación DIGSA
	PD. Silvestre Granados Silva Coordinador Grupo Gestión de la Información DIGSA	TAST. Yamile López Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones PROGTIC Gestora de Calidad
	SMSM. Adriana Espinel Torres Grupo Planeación Estratégica DIGSA Área Sistemas Integrados de Gestión PROASIG	PD. Alexandra Martínez Vargas Coordinadora Grupo Planeación Estratégica DIGSA Representante de la Alta Dirección
Elaboró:	PD. Alexandra Mora Nova Grupo Gestión de la Información DIGSA Área Coordinación y Suministro de Información	PD. Julio Cesar Salgado Guerrero Grupo Sistema Integral De Información – Tecnologías De La Información Y Las Comunicaciones - SISAM Área Administración Del Sistema Y Base De Datos

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

Presentación PETI 2023-2026 V5

La Dirección General de Sanidad Militar, en concordancia con las políticas de Seguridad, Defensa y Convivencia Ciudadana 2022–2026 “Garantías para la Vida y la Paz” y el Plan Nacional de Desarrollo 2022–2026 “Colombia, Potencia Mundial de la Vida”, así como en alineación con el Plan Estratégico de Tecnologías de la Información del Sector Defensa y Seguridad 2023–2026 y las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones, establece criterios institucionales para la estandarización de todos los temas relacionados con las Tecnologías de la Información y las Comunicaciones (TIC).
Este enfoque busca integrar de manera eficiente las TIC, fortalecer capacidades institucionales, implementar mecanismos de uso y apropiación tecnológica, y optimizar los procesos internos de la Dirección. Asimismo, se promueve el establecimiento de herramientas de control que permitan la 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 los mismos 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.

1 Plan Nacional de Desarrollo 2022 – 2026 “Colombia, Potencia Mundial de la Vida”, 3 de mayo de 2023
2. https://www.gsed.gov.co/ministerio/centro-de-documentos/politicas-sectoriales/plan-estrategia-de-tecnologias-de-informacion

1. Objetivo del documento

Contar con un Plan Estratégico de Tecnologías de la Información (PETI 2023-2026) de la Dirección General de Sanidad Militar para integrar y ejecutar iniciativas de Tecnologías de la Información y Comunicaciones (TIC) alineadas con la Estrategia Institucional, el Gobierno de Datos y la Transformación Digital, para fortalecer y actualizar la base tecnológica y de comunicaciones, para garantizar la Prestación de Servicios de Salud del SSFM.

2. Alcance del PETI

El Plan Estratégico de Tecnologías de la Información y Comunicaciones 2023 – 2026 V5, incluye para su construcción y ejecución los Grupos de trabajo de la DIGSA (ver anexo de soportes de asistencia), 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).

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

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

- 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 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 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 2194 de 2017, "Decreto modificatorio del artículo 2.2.2.4.1 del Decreto ÚnicoReglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto número 1078 de 2015".

- Decreto 612 de 2018, "Por el cual se fijan directrices para la integración de los planesinstitucionales 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 desalud 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 laTecnología de la información y las comunicaciones, con el fin de definir lineamientosy estándares aplicables a la Transformación Digital Pública".
- Decreto 767 de 2022, por el cual se establecen 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 del 2015

- Decreto 338 de 2022, por medio del cual se estable los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras criticas cibernéticas y servicios esenciales, la gestión del riesgo y las respuestas a incidentes de Seguridad Digital.

- Decreto 088 de 2022, Establece los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea

- Decreto 338 de 2022, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones

- Resolución 3374 de 2000, “Por la cual se reglamentan los datos básicos que debenreportar 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 Tecnologíasde Información y Comunicaciones – CITI – del Sector Defensa, para fijar las políticasde estandarización en materia de tecnología, comunicaciones y servicios en el Ministerio de Defensa Nacional”.

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

- 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 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 1126 de 2021, las entidades territoriales deben finalizar la adopción del protocolo IPv6 a más tardar el 31 de diciembre de 2022. Lo anterior en virtud de la necesidad de ofrecer más y mejores servicios en internet.

- Resolución 460 de 2022, Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.

- 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 oDependencias 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 Integral de Salud de las Fuerzas Militares y de la Policía Nacional”.

- Circular 12 de 2007, “Verificación, recomendaciones, seguimiento y resultados sobreel cumplimiento de las normas en materia de derechos de autor sobre programas decomputador”.

- 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 bajolos 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; definelos 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 devida 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”.

4. 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

Amenaza informática: es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

Análisis de datos: consiste en cuestionar los datos para encontrar información útil.

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

Analítica de datos: hace referencia a un examen sistemático de datos que incluye todas las tareas asociadas, tales como: recopilar o cargar datos; categorizarlos en formas estructuradas o no estructuradas; almacenarlos y gestionarlos, normalmente en bases de datos, lagos de datos y/o almacenes de datos; transformarlos y analizarlos para extraer patrones, tendencias y conocimientos; y compartirlos con usuarios o partes interesadas, a menudo mediante un panel de control o a través de un medio de despliegue específico.

Analítica de datos avanzada: manera de utilizar datos que no habían sido explotados previamente, tanto de fuentes cualitativas como cuantitativas, de forma independiente, o junto con datos existentes, para extraer nuevos conocimientos que permitan mejorar y agilizar la toma de decisiones. Se basa en instrumentos que facilitan el análisis estadístico, favoreciendo la utilización de distintos tipos de modelos de predicción y prescripción. Si bien no existe una frontera específica que marque la diferencia entre la analítica tradicional y la avanzada, esta última se distingue por la utilización de herramientas estadísticas más complejas, minería de datos, procesos estocásticos y algoritmos matemáticos.

Analítica de datos descriptiva: orientada a describir o narrar la realidad de un sector o negocio y su entorno. Incluye los análisis que intentan explicar las causas.

Arquitectura actual AS-IS: es el análisis de la situación actual de la Entidad u organización a partir de los dominios o dimensiones (Institucional, Información, Sistemas de Información, Tecnología y Seguridad).

Arquitectura de datos: una descripción de la estructura y la interacción de los principales tipos y fuentes de datos, activos de datos lógicos, activos de datos físicos y recursos de gestión de datos.

Arquitectura empresarial: es una práctica estratégica que consiste en analizar integralmente las entidades desde diferentes perspectivas o dimensiones, con el propósito de obtener, evaluar y diagnosticar su situación actual y establecer la transformación necesaria. El objetivo es generar valor a través de las Tecnologías de la Información para que se ayude a materializar la visión de la entidad.

Arquitectura de información: disciplina encargada del estudio, análisis, organización, disposición y estructuración de la información. Arquitectura de Tecnología También es conocida como Arquitectura de servicios tecnológicos. Incluye todos los elementos de TI que soportan la operación de la institución, entre los que se encuentran la plataforma hardware, la plataforma de comunicaciones y el software especializado (sistema operacional, software de comunicaciones, software de integración y manejadores de bases de datos, software de seguridad, entre otros).

Authenticator: es un software basado en autenticación con contraseña de un solo uso desarrollado por Google. Google Authenticator ofrece un número de seis dígitos que el usuario debe proporcionar además de su nombre de usuario y contraseña para acceder a los servicios de Google

Brecha digital: hace referencia a la diferencia socioeconómica entre aquellas comunidades que tienen accesibilidad a las TIC y aquellas que no, y también hace referencia a las diferencias que hay entre grupos según su capacidad para utilizar las TIC de forma eficaz, debido a los distintos niveles de alfabetización y capacidad tecnológica.

Calidad de datos: es la cualidad de un conjunto de información que reúne atributos como la exactitud, integridad, coherencia, relevancia, accesibilidad y confiabilidad necesarias para el procesamiento y análisis.

Cibercrimen (delito cibernético): conjunto de actividades ilegales asociadas con el uso de las TIC, como fin o como medio.

Ciberseguridad: es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio.

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.

Data lake: su significado en castellano es “lago de datos” y es el repositorio donde se almacenan los datos en bruto de una organización. Aunque la información no se encuentre necesariamente estructurada ni el dato preparado para su empleo, es necesario implementar un catálogo de la información recogida, normas de trazabilidad de los datos, una estrategia de seguridad de los mismos y la conexión con las herramientas de uso posterior para procesar, analizar o aplicar inteligencia artificial.

Data mart: es un subconjunto de un Data Warehouse orientado al análisis, almacenamiento e integración de los datos de un área de la empresa.

Data warehouse: un data warehouse desempeña un papel central en los sistemas de Business Intelligence al recopilar, integrar y analizar datos provenientes de diversas fuentes de datos. Se trata de un entorno de integración de datos que combina tecnologías y componentes para almacenar, consultar y analizar grandes volúmenes de datos, transformándolos en información valiosa y accesible para los usuarios.

Dato: es una representación simbólica de una característica de un elemento o situación, que pertenece a un modelo de una entidad.

Dato maestro: datos sobre las entidades del mundo real (personas, organizaciones, lugares u objetos) que proporcionan contexto para los registros administrativos, transacciones y análisis que realiza la institución y, por ende, que comparte toda la entidad. Por su naturaleza prácticamente nunca son datos transaccionales.

Datos abiertos: son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos estructurados: los datos estructurados tienen un formato estandarizado que permite tanto al software como a las personas acceder a estos de forma eficaz. Por lo general, se trata de datos tabulares con filas y columnas que definen claramente sus atributos. Las computadoras pueden procesar eficazmente los datos estructurados en busca de información dado que se trata de información cuantitativa.

Datos no estructurados: aquellas colecciones grandes de datos que no se almacenan en un formato de base de datos estructurada. Tienen estructura interna, pero no están predefinidos por los modelos de datos. Pueden ser de cualquier índole: multimedia, imágenes, audio, datos de sensores, textos y otros. No se deben confundir con aquellos que no están preparados para su uso.

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

Establecimiento de sanidad militar (ESM): es el encargado de la prestación de servicios de salud a todos los usuarios del SSFM de acuerdo a su portafolio de servicios, solucionando la demanda de servicios ambulatorios remitidos de otro ESM o de la red externa, ejecuta actividades de vigilancia epidemiológica, promoción y prevención, observación y/o aislamiento de pacientes, encaminadas a satisfacer la demanda propia de cada especialidad, será punto de recepción, evaluación y estabilización en urgencias o atención médica odontológica priorizada.

Estadística oficial: estadísticas producidas y difundidas por las entidades integrantes del Sistema Estadístico Nacional que permiten conocer la situación económica, demográfica, ambiental y social a nivel nacional y territorial para la toma de decisiones y que cumplen las condiciones y características establecidas en el artículo 2.2.3.2.1 del Decreto 1743 de 2016. se consideran estadísticas oficiales, aquellas producidas y difundidas por las entidades integrantes del Sistema Estadístico Nacional (SEN), que permiten conocer la situación económica, demográfica, ambiental, social, y cultural de acuerdo con el nivel de desagregación territorial de la operación estadística, para la toma de decisiones. También constituyen estadísticas oficiales, las producidas por el Departamento Administrativo Nacional de Estadística — DANE en el cumplimiento de sus funciones.

Fichas técnicas de indicadores: es un documento en que se detallan las características y variables para realizar una comparación entre dos o más tipos de datos que sirve para elaborar una medida cuantitativa o una observación cualitativa.

Firma digital: es el valor numérico que se adhiere a un mensaje de datos y que utiliza un procedimiento matemático conocido vinculado a la clave del iniciador y al texto del mensaje para determinar que este valor se haya obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no haya sido modificado después de efectuada la transformación.

Firma electrónica: la firma electrónica corresponde a métodos tales como códigos, contraseñas, datos biométricos o claves criptográficas privadas, que permitan identificar a una persona en relación con un

mensaje, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, teniendo en cuenta todas las circunstancias del caso, así como cualquier acuerdo pertinente.

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.

Hackear: es el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar información, suplantar la identidad del dueño, beneficiarse económicamente o protestar.

Hallazgo: son hechos o situaciones que denotan importancia por la forma como repercuten en la administración, incidiendo en el cumplimiento de la misión de la SDS; estos se clasifican en no conformidades cuando se contraviene un requisito legal y oportunidad de mejora; Cuando la actividad no tiene incidencia legal, pero es susceptible de avance.

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.

Inteligencia artificial: es la habilidad de una máquina para imitar el funcionamiento de la mente humana con acciones como el razonamiento, el aprendizaje, la creatividad o la planificación.

Inteligencia de negocios – BI: tipo de análisis de datos destinado a comprender las actividades y oportunidades de las entidades. Los resultados de dicho análisis se utilizan para mejorar el éxito de las entidades.

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.

IoT o internet de las cosas: se conoce así a la conexión de los objetos físicos a Internet para la transmisión e intercambio de datos.

Kactus: software de nómina que permite gestionar, controlar y optimizar los procesos de talento humano.

Maltrato la**b**oral TI: es todo a**c**to de violencia contra la integ**r**idad física o moral, la libertad física **o** sexual y los bienes de quien se desempeñe **c**omo empleado o funcionario; l**a**s exp**r**esiones verbales injuriosas o ultrajant**e**s que lesione la integridad moral o los derechos a la intimidad y al buen nombre de quienes participen en una relación de trabajo de tipo laboral o todo comportamiento tendiente a menoscabar la autoestima y la dignidad de quien participe en una relación de trabajo de tipo laboral.

Malware: el malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer acciones delictivas.

Mantenimiento correctivo: es la revisión destinada a las correcciones de defectos observados en los vehículos y consiste en localizar averías, defectos y corregirlos o repararlos por mal funcionamiento. Por su naturaleza no pueden planificarse en el tiempo, presenta costos por reparación y repuestos no presupuestados, pues puede implicar el cambio de algunas piezas del equipo en caso de ser necesario.
Mantenimiento preventivo: es la revisión destinada a la conservación de equipos o instalaciones mediante la realización de una inspección que garanticen el buen funcionamiento y fiabilidad en prevención de fallas que puedan aparecer en el futuro.

Nube: término usado para referirse a la computación en la nube (cloud computing). Trata de los servicios en la web que proveen características básicas y avanzadas de procesamiento y almacenamiento.

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.

Sandbox: en informática, el término caja de arena (traducción al castellano) se refiere a un entorno aislado de pruebas en el que se testean desarrollos antes de su integración en un sistema. En Big Data, estos entornos aislados se emplean como espacios para la exploración colaborativa de datos y son plataformas con gran capacidad de gestión y procesamiento de datos que se emplean para la experimentación con grandes volúmenes de datos.

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.

Transformación digital: es el proceso mediante el cual una organización integra tecnología digital a todas las áreas de la entidad. Este proceso cambia por completo la forma en que una entidad ofrece valor a los clientes. Comprar equipos de cómputo y software NO es transformación digital.

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

X-Road: es un software de código abierto que permite a instituciones y organizaciones intercambiar información a través de Internet. X-Road constituye una capa de integración y los diferentes tipos de integraciones, distribuida entre sistemas de información, que proporciona un modo estandarizado y seguro de desplegar y utilizar servicios.

5. Acrónimos

DIGSA	Dirección General de Sanidad Militar
ESM	Establecimientos de Sanidad Militar
GRTIC	Grupo de Tecnologías de la Información y las Comunicaciones
GRUPL	Grupo Planeación Estratégica.
LAN	Red de área Local
MINTIC	Ministerio de Tecnología de la Información y las Comunicaciones
PEI	Plan Estratégico Institucional
PROGTIC	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones.
PROGI	Proceso Gestión de la Información.
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.
SISAM	Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones.
SSMP	El Sistema de Salud de las Fuerzas Militares y de la Policía Nacional
SUBTG	Subdirección técnica y de Gestión
TIC	Tecnología de la información y las Comunicaciones
WAN	Red de área amplia

6. Marco Conceptual

El Plan Estratégico de Tecnologías de la Información (PETI) de la Dirección Nacional de Sanidad Militar (DIGSA), refleja el ejercicio realizado por la Subdirección Técnica y de Gestión (SUBTG) para la planeación de las adquisiciones, desarrollo, soporte, mantenimiento, uso y apropiación de las tecnologías de la información, con el objetivo de asegurar que las metas y objetivos de TI, estén vinculados y alineados con las metas y objetos de la Entidad.

El PETI es dinámico, se adapta a los cambios en el entorno, a las regulaciones, normas y metodologías aplicables del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y Ministerio de defensa, está formulado para la vigencia 2023 – 2026, con versión de actualización cada año, alineado mediante los Motivadores Estratégicos: Estrategia Nacional, Estrategia Sectorial, Estrategia Institucional y Lineamientos y Políticas.

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

Fuente GRUGI 2024

Tabla 1. Motivadores Estratégicos

Motivador	Fuente
Estrategia Nacional	Plan Nacional de Desarrollo de Colombia 2022-2026 “Colombia potencia de la vida”, contiene motivadores estratégicos para la definición del PETI, los cuales se definen en los Componente de transformación **# 2** Seguridad humana y justicia social y el componente de transformación **# 9**: Legitimidad, transparencia e integridad de las instituciones para la seguridad humana ítem b. Sistema de Bienestar Integral de la Fuerza Pública, sus familias y de los veteranos.
Estrategia Sectorial	El Plan Estratégico Institucional para el Sistema de Salud de las Fuerzas Militares y de la Policía Nacional 2023-2026 (PEI SSMP 2023- 2026) se encuentra perfectamente alineado y en concordancia con el Plan Nacional de Desarrollo 2022-2026, la Política de Seguridad, Defensa y Convivencia Ciudadana para la protección de la vida 2022-2026 (PSDCC), la Política Integral de Bienestar para la Fuerza Pública y sus familias 2023-2026, y, finalmente, el Plan Estratégico Sectorial de Defensa 2023- 2026. Esta alineación se refleja tanto en el ámbito de aplicación como en la coherencia con los objetivos, planes, programas y estrategias del Sistema de Salud de las Fuerzas Militares y de la Policía Nacional.
Estrategia Institucional	La construcción del Plan Estratégico Institucional PEI 2023 - 2026 se proyectó de manera participativa en diversas mesas de trabajo con la Dirección de General de Sanidad Militar, Sanidad Ejército Nacional, Sanidad Naval y la Jefatura de Salud de la Fuerza Aérea, con el fin de identificar cada una de las iniciativas estratégicas, acciones, actividades estratégicas y productos del Subsistema de salud de las Fuerzas Militares. En el marco de la alineación estratégica, El PEI 2023-2026; impulsa la **Iniciativa 1**. Mejoramiento en la Rectoría y Gobernabilidad del SSMP – Acción 1.3: Documento "**Modelo de gobierno de datos**" para la planeación y modernización del Subsistema de Salud de las FFMM y hoja de ruta para la implementación y la **Iniciativa 6**. Desarrollar e implementar un Sistema de Información en Salud funcional, acorde con las necesidades de cada Subsistema de Salud, con la modernización de las plataformas tecnológicas actuales para una óptima administración y gerenciamiento del Sistema. - Acción 6.1: Actualizar el proyecto de inversión para el fortalecimiento y modernización del Sistema de información en salud del SSFM **- Adoptar la transformación digital en cumplimiento a la política de gobierno digital**
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.

Motivador	Fuente
	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 0Fuerzas Militares y la Policía Nacional para la salud deberán manejarse en fondos

Motivador	Fuente
	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.

Fuente: Elaboración propia GRUGI

7.2. Tendencias Tecnológicas

Tabla 2. Tendencias Tecnológicas

Nombre	Descripción Actual 2024
Aplicaciones móviles	Aplicación sincronizada con Office 365 estas aplicaciones son básicamente herramientas colaborativas, las cuales se pueden sincronizar tanto en pc como en dispositivo móvil con licencia activa (authenticator, Temas, Word, Excel, Power Point, Planner, To Do, Power Apps, Power Bi, Delve entre otras). 2. Eshare: Aplicación de Pantalla Interactiva (Ayudantía). Lo anterior permite portabilidad para el uso de las herramientas ofimáticas anteriormente mencionadas, permitiendo el acceso desde cualquier ubicación en el territorio nacional, solo se requiere accesos a internet. Adicionalmente cuentan la aplicación Authenticator que suministra una capa de seguridad adicional para la autenticación de los usuarios en la nube Office 365.

Nombre	Descripción Actual 2024
Uso de nube- Software como servicio - Microsoft 365.	Se dispone de Microsoft 365 con acceso a aplicaciones de productividad y colaborativa como son Microsoft Word, Excel, Power Point, Access, Teams, además servicios de correo electrónico institucional.
Uso de nube- Plataforma como servicio	1. La herramienta DevOps integra desarrollo de software (Dev) y operaciones de TI (Ops) para mejorar la colaboración y la eficiencia en la entrega de software. 2. Azure
Uso de nube- Infraestructura como servicio	Se tiene el servicio de créditos en nube donde se encuentra alojado el Directorio Activo, como medida de prevención: La Dirección General de Sanidad Militar tiene implementado un enfoque de seguridad por capas. Este enfoque está basado en la utilización de soluciones de Palo Alto Networks, incluyendo Córtex/XDR, Firewall, FortiMail de palo Alto. Proporcionando una protección unificada contra amenazas, integrando datos de red, endpoint y nube. El Firewall de Palo Alto garantiza la seguridad de la red en entornos virtuales y en la nube, mientras que FortiMail protege contra amenazas por correo electrónico, esta combinación de soluciones ofrece una defensa robusta y proactiva contra-ciberataques. Así mismo se utiliza la herramienta WSUS, el correlacionado SIEM ubicado en la DIGSA el cual se desplegó en los activos de información enviando logs de eventos al servidor de FORTISIEM del CCOCI, para un monitoreo constante de vulnerabilidades, y por último la configuración del doble factor de autenticación de todos los usuarios del correo electrónico Institucional que en la actualidad se encuentra integrado con el Directorio Activo y sincronizado híbridamente en Híper-V con créditos en la nube. De esta manera se garantiza la alta disponibilidad y se fortalece la seguridad de la infraestructura tecnológica de la DIGSA. Y así mismo con el despliegue de la licencia de Vicarius VRX, se mejora la seguridad tecnológica y se fortalece la estabilidad operativa en la DIGSA al ofrecer análisis de vulnerabilidades y remediación en tiempo real. La licencia de Vicarius VRX proporciona agentes instalados en cada endpoint, servidor y componente de la infraestructura tecnológica, lo que permite una supervisión continua y una respuesta inmediata a amenazas. Con una plataforma centralizada independiente para cada grupo de activos, se optimiza la protección y gestión de la seguridad en toda la infraestructura. Vicarius VRX tiene la capacidad para identificar y solucionar problemas de seguridad, reduciendo riesgos de la DIGSA.
Automatización de procesos con motor RPA (Robotic Process Automation)	1. Automatización en la extracción de información de historias clínicas, para la construcción del reporte cuenta de alto costo. 2.Flujos automatizados para gestión de notificaciones en las aplicaciones construidas.
Software para análisis de datos predictivo	1. SAP(Local) 2. Power BI
Máquinas virtuales (Virtualización de hardware)	Migración de máquinas virtuales en ambiente Vmware al Sistema Microsoft Hyper-V,

Nombre	Descripción Actual 2024
Devops	Licencias, se dispone de licencia para programar desarrollos de software onpremise, se utiliza dentro del proceso de Fabrica de Software.
Plataforma de interoperabilidad X-ROAD	En este momento hay interoperabilidad con hospital militar bajo el estándar HL7 FHIR Fast Healthcare Interoperability Resources
Ciberseguridad	Contrato Actual en ejecución No. 167-DIGSA-2024 Suministrar, instalar, configurar y poner en funcionamiento infraestructura de Telecomunicaciones, y poner en funcionamiento e implementar servicios de un centro de operaciones de Red (NOC) y un Centro de operaciones de seguridad (SOC) para la Dirección General de Sanidad Militar. Asimismo, se tiene implementados actualmente los siguientes aspectos en materia de Ciberseguridad. 1). Capacitación y Concienciación: Programas de formación para empleados sobre ciberseguridad y buenas prácticas. 2). Control de Acceso: Sistemas que limiten el acceso a la información y recursos a personal autorizado, desde el Directorio Activo, Firewall y referente a correo las herramientas con las que cuenta Office 365 para correo electrónico. 3). Monitorización y Detección: Herramientas como Firewall, Antivirus XDR Cortex y FortiMail para supervisar redes, correo y sistemas en busca de actividades sospechosas. 4). Copias de Seguridad: Se realizan respaldos regulares de los ambientes de producción y la data de la Entidad. 5). Colaboración Interinstitucional: Mecanismos para compartir información sobre amenazas y buenas prácticas con otras entidades públicas del mismo sector defensa. 6). Se implemento la instalación de los agentes VICARIUS para mitigar las vulnerabilidades y automatizar la instalación de parches para el sistema operativo.

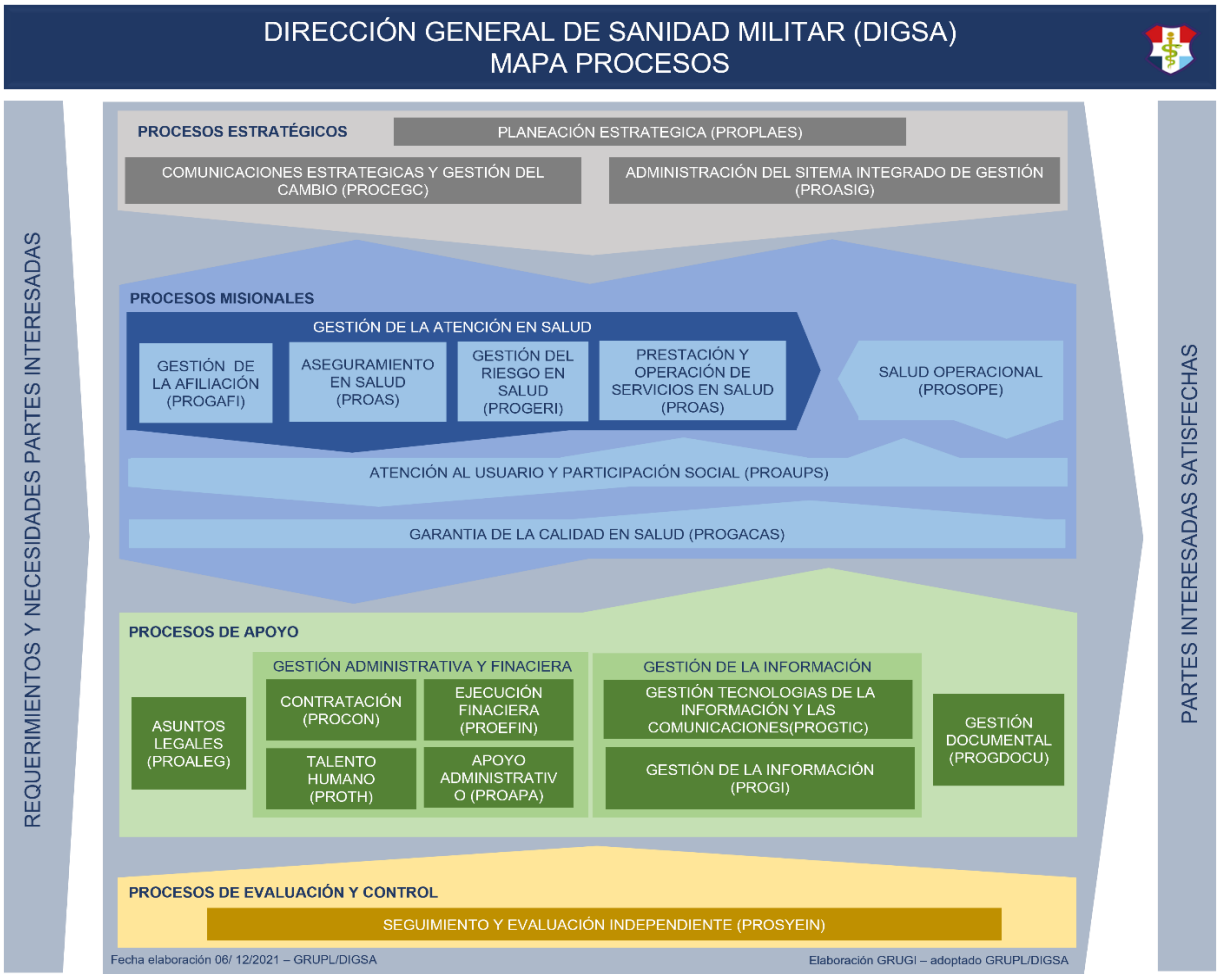
Fuente: Elaboración propia SISAM

7. Modelo Operativo

Para los procesos operativos 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 así:

- Procesos Estratégicos
- Procesos Misionales
- Procesos de Apoyo
- Procesos de Evaluación y Control

Ilustración 2. Mapa de Procesos DIGSA



Fuente: Elaboración propia GRUGI

7.3. Descripción de procesos

7.3.1. Procesos estratégicos

Tabla 3 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.

Abreviación	Nombre	Objeto
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 tecnológicas:

- Portal Web y Portal SaludSIS: Portal de trámites en línea para el Subsistema de Salud de las Fuerzas Militares, utiliza canales de comunicación oficiales de la Entidad, de cara al ciudadano, usuarios afiliados y sus familias, ofrecen servicios y tramites en línea. Siendo un instrumento de aplicación de las políticas de Gobierno Digital.

- Suite Visión Empresarial: permite controlar los documentos y hacer seguimiento a indicadores, planes de acción, auditorias, acciones correctivas, preventivas, ideas de mejora etc.

- SGDEA: El sistema de gestión documental y especialmente el sistema de gestión documental electrónica, que se convierte en el repositorio de todos aquellos documentos electrónicos de archivo generados por las entidades, se encuentra descrito, definido y caracterizado en las siguientes normas

7.3.2. Procesos misionales

Tabla 4 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.
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

Abreviación	Nombre	Objeto
		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.

- 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.

7.3.3. Procesos de apoyo

Tabla 5 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

Abreviación	Nombre	Objeto
		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: Es el Software de Nómina integral (Remuneración, Compensación y Nomina electrónica) que permite gestionar, monitorear y optimizar los recursos de la entidad.

- 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, Dinámica Gerencial es un sistema de información modular, que se integra a través de subsistemas totalmente en línea, las áreas administrativas, financieras, asistenciales y operativas de las instituciones de salud.

- SECOP: Es una plataforma para realizar todo el Proceso de Contratación en línea. Desde la cuenta de la Entidad Estatal puede crear y adjudicar Procesos de Contratación, registrar y hacer seguimiento a la ejecución contractual. Los Proveedores también tienen su cuenta, desde la cual envían observaciones y ofertas. Se trata de un sistema transaccional cero papeles.

- SIIF Nación: El Sistema Integrado de Información Financiera (SIIF) Nación es una herramienta modular, transversal y transaccional, a través de la cual las entidades que hacen parte del Presupuesto General de la Nación realizan su gestión financiera pública, de manera estandarizada, segura, conforme a la norma en línea y tiempo.

- ERP-SAP: sistema que estandariza, unifica y automatiza sobre una plataforma tecnológica moderna y de última generación, los procesos administrativos de tipo logístico en la gestión de compras, gestión de inventarios y de almacenes, gestión de tipo financiero en los procesos contables, de tesorería, activos fijos y de costos, la gestión de mantenimiento de equipos propios de la Fuerza Pública. Adicionalmente, soportado por un área de operación SILOG se encuentra implementado sobre la plataforma tecnológica SAP 7, soportado sobre una infraestructura de hardware y unos criterios de arquitectura de solución para gestión de seguridad de la información.

7.3.4. Proceso de evaluación y control

Tabla 6 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

7.3.5. Alineación de TI con los procesos

Teniendo en cuenta la caracterización de los procesos y su relación con los Sistema de Información, a continuación, se relacionan los Sistema de Información que brindan soporte a las actividades para el cumplimiento de los objetivos de cada proceso, indicando el tipo de cubrimiento Total, Parcial o si no se cuenta con el Apoyo.

ID	Proceso	Categoría	Sistema de Información	Cubrimiento
001	Aseguramiento en Salud – PROAS Prestación y Operación de Servicios de Salud – PROAS Garantía de la Calidad – PROGACAS Salud Operacional – PROSOPE Gestión de Riesgo en Salud – PROGRERI	Misional	Sistema integral de información del SSFM SALUD.SIS	Total
			Sistema Cuenta de Alto Costo	Parcial
			Seguimiento a Casos de COVID-19 MINSALUD - SegCovid19	Parcial
			SISMUESTRAS Registro Nacional de pacientes y resultados INS	Parcial
			PISIS - Plataforma de transporte de información MINSALUD	Parcial
			PAIWEB - MINSALUD	Parcial
			SICAD – Catalogación MINDEFENSA	Parcial
			RedDataINS	Parcial
			Sistema de Rendición Electrónica de la Cuenta e Informes - SIRECI	Parcial
			Sistema Nacional de Vigilancia en Salud Pública -SIVIGILA	Parcial
			Sistema de Peticiones, Quejas y Reclamos – Supersalud - SUPERSALUD	Parcial
			Administradora de los Recursos del Sistema General de Seguridad Social en Salud - ADRES	Parcial
002	Gestión de la Afiliación - PROGAFI	Misional	Sistema integral de información del SSFM SALUD.SIS	Total
			Sistema de Gestión de Documento Electrónico de Archivos SGDA	Parcial

ID	Proceso	Categoría	Sistema de Información	Cubrimiento
			Software de Gestión de Portafolio de Proyectos Suite Visión Empresarial	Parcial
003	Asuntos Legales - PROALEG	Estratégico	Sistema de Gestión de Documento Electrónico de Archivos SGDA	Parcial
			Software de Gestión de Portafolio de Proyectos Suite Visión Empresarial	Parcial
004	Comunicaciones Estratégicas y Gestión del Cambio - PROCEGC	Estratégico	Página WEB	Total
			Sistema de Gestión de Documento Electrónico de Archivos SGDA	Parcial
			Software de Gestión de Portafolio de Proyectos Suite Visión Empresarial	Parcial
005	Planeación Estratégica – PROPLAES	Estratégico	Sistema integral de información del SSFM SALUD.SIS	Parcial
			Sistema de Gestión de Documento Electrónico de Archivos SGDA	Parcial
			Software de Gestión de Portafolio de Proyectos Suite Visión Empresarial	Parcial
			Sistema Integrado de Información Financiera - SIIF Nación	Total
			Plataforma Integrada de Inversión Pública - PIIP	Total
			Plataforma para Trámites administrativos - BIZAGI	Total
			Sistema de Administración de Recursos Financieros ERP-SAP	Total
			Formulario Único de Reporte de Avances de la Gestión (FURAG)	Parcial
			Sistema Único de Tramites y Servicios - SUIT	Parcial
006	Administración del Sistema Integrado de Gestión - PROASIG	Estratégico	Sistema de Gestión de Documento Electrónico de Archivos SGDA	Parcial
			Software de Gestión de Portafolio de Proyectos Suite Visión Empresarial	Parcial
007	Gestión Documental - PROGDOCU	Apoyo	Sistema de Gestión de Documento Electrónico de Archivos SGDA	Total
			Software de Gestión de Portafolio de Proyectos Suite Visión Empresarial	Parcial
008	Talento Humano - PROTH	Apoyo	Sistema de Administración del Talento Humano (KACTUS)	Total
			Sistema de recursos humanos y nómina KACTUS-OPHELIA	Total
			Sistema de Gestión Documental (ONBASE)	Parcial
			Sistema de Gestión de Documento Electrónico de Archivos SGDA	Parcial
			Sistema de Información y Gestión del Empleo Público (SIGEP)	Parcial
			Software de Gestión de Portafolio de Proyectos Suite Visión Empresarial	Parcial
			Página WEB	Parcial

ID	Proceso	Categoría	Sistema de Información	Cubrimiento
009	Contratación - PROCON	Apoyo	Sistema Electrónico para la Contratación Pública – SECOP	Total
			Tienda Virtual del Estado Colombiano	Total
			Sistema de Rendición Electrónica de la Cuenta e Informes - SIRECI	Parcial
010	Ejecución Financiera	Apoyo	Sistema de Rendición Electrónica de la Cuenta e Informes - SIRECI	Parcial
			Sistema Electrónico para la Contratación Pública – SECOP	Parcial
			Sistema Integrado de Información Financiera - SIIF Nación	Total
			Circular Única - SUPERSALUD	Parcial
			Sistema Consolidador de Hacienda e Información Pública - SCHIP	Parcial
011	Gestión de la Información y la Comunicaciones – PROGTIC	Apoyo	Sistema de Gestión de Documento Electrónico de Archivos SGDA	Parcial
			Plataforma de Seguridad (PALO ALTO)	Total
			FIREWALL-CORTEX/XDR-FORTIMAIL	Total
			SOC-NOC	Total
			VICARIUS/VRX	Total
			MICROSOFT 365	Total
			ANTIVIRUS CORTEX	Total
			Software de Gestión de Portafolio de Proyectos Suite Visión Empresarial	Parcial
			Sistema integral de información del SSFM SALUD.SIS	Total
012	Apoyo Administrativo - PROAPA	Apoyo	Sistema de Gestión de Documento Electrónico de Archivos SGDA	Parcial
			Software de Gestión de Portafolio de Proyectos Suite Visión Empresarial	Parcial
			Sistema Integrado de Información Financiera - SIIF Nación	Total
013	Gestión de la Información - PROGI	Apoyo	Sistema de Gestión de Documento Electrónico de Archivos SGDA	Parcial
			Power Platform(Power Apps, Sharepoint, Power Bi, Power Automate)	Tota
			Software de Gestión de Portafolio de Proyectos Suite Visión Empresarial	Parcial
			Sistema integral de información del SSFM SALUD.SIS	Total
014	Seguimiento y Evaluación Independiente - PROSYEIN	Evaluación y Control	Sistema de Administración de Recursos Financieros ERP-SAP	Total
			Sistema Consolidador de Hacienda e Información Pública - SCHIP	
			Software de Gestión de Portafolio de Proyectos Suite Visión Empresarial	Parcial
			Sistema de Gestión de Documento Electrónico de Archivos SGDA	Parcial

Fuente: Elaboración propia SISAM

7.3.6. Servicios institucionales

ID	001	
Nombre	Gestión de Afiliación y tramites en Salud	Oportunidades de mejora con TI
Descripción	Registro de Afiliación, Actualización de Datos, Agendamientos de Citas, Encuestas de Satisfacción, Historia Clínica, Autorizaciones, Cuentas Medicas)	• Acceso por canal app móvil • Servicio totalmente online • Gestión de Citas automatizada • Revisar Criterios de Usabilidad y Accesibilidad.
Horario de Prestación	Horario 7/24 Procesos en línea Presencial 8 Horas 5 días a las Semana	
Usuario Objetivo	Personal Militar, Beneficiarios	
Canal de Acceso	Correo Electrónico Formulario Físico Canal WEB Pagina Institucional Presencial	

7.3.7. Trámites

ID	001	
Nombre	Registro de afiliación al Subsistema de Salud de las Fuerzas Militares	Oportunidades de mejora con TI
Descripción	Obtener la afiliación al Subsistema de Salud de las Fuerzas Militares como titular y el de su núcleo familiar	• Acceso por canal app móvil • Servicio totalmente online • Gestión de Citas automatizada • Revisar Criterios de Usabilidad y Accesibilidad.
Horario de Prestación	Horario 7/24 Procesos en línea Lunes a viernes 8:00 am a 5:00 pm jornada continúa	
Usuario Objetivo	Personal Militar, Beneficiarios	
Canal de Acceso	Correo Electrónico Formulario Físico Canal WEB Pagina Institucional Presencial	

8. SITUACIÓN ACTUAL

8.1. 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.

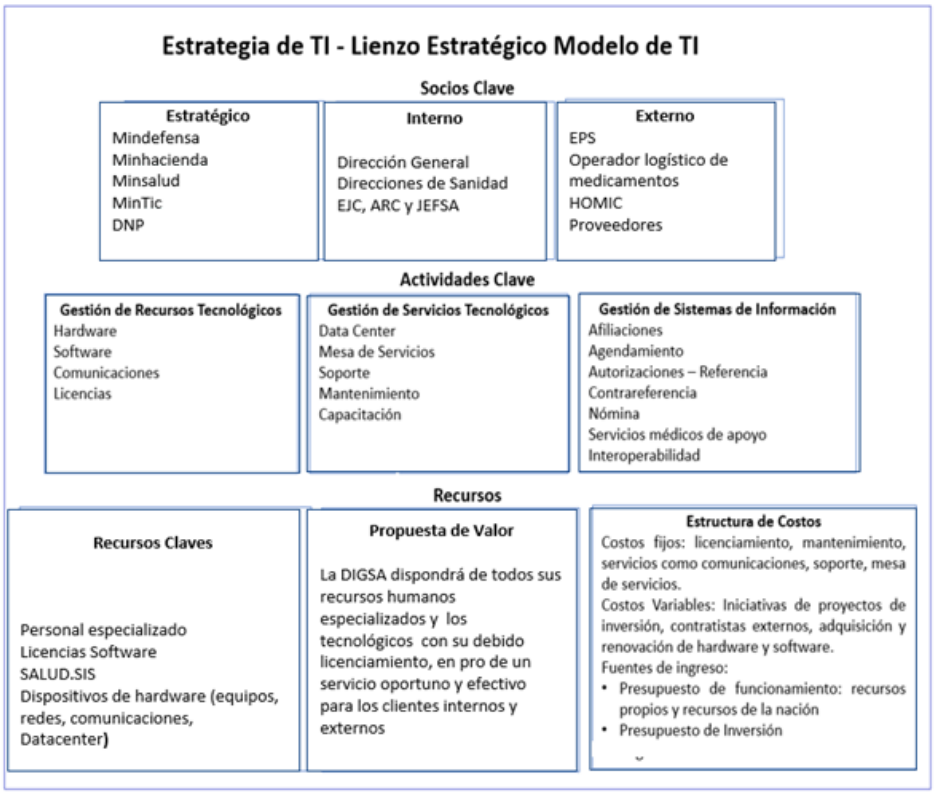
La Estrategia de TI utilizada para desarrollar las políticas y lineamientos de las tecnologías de la información del Subsistema de Salud está enmarcada en la Directiva No. 20036 del 01 de noviembre de 2018 "Impartir las instrucciones para la continuidad del desarrollo y culminación de la implementación 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.

8.1.1. 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



Fuente: Elaboración propia SISAM

8.1.2. 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.

8.1.3. 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.

8.1.4. 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.

Tabla 7 Matriz DOFA

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,	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.

ENTORNO INTERNO	
FORTALEZAS	**DEBILIDADES**
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.	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.	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.

ENTORNO INTERNO	
FORTALEZAS	**DEBILIDADES**
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	A5. Existencia de equipos de cómputo con tecnología avanzada para la agilidad en los diferentes procesos.

Fuente: Elaboración propia GRUGI

8.1.5. 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 8 servicios TI

Servicios	Descripción
Puestos de Trabajo	Suministro componentes informáticos requeridos para un puesto de trabajo: Escritorio, silla, ergonómica, Punto de Red, canaleta de red eléctrica, Hardware (CPU, monitor, mouse, teclado, Scanner, diadema, teléfono, extensión). Correo, licencias, SharePoint, 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 365 (Ofimática, One drive, SharePoint, Power Apps, One Note, To Do, Planner, Teams, entre otros…)
Aplicativos misionales	Portal Salud SIS
Aplicativos de Apoyo	Kactus, On base y visual médica, Power Apps
Aplicativos de Servicio	Plataforma seguridad (Palo Alto) - Cortex XDR -FORTIMAIL– END POINT- NOC- SOC , Azure Connection-colección de servidores y hardware de red.
Software de Terceros	SGDA- proporcionada por COMANDO 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 9 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.	
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 10 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

Atributo	Descripción	
	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	
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 11 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	
	Desarrollo Externo	X
	Adquirido sin modificaciones	
	Adquirido con modificaciones	
	Software como servicio	
Fabricante	Hyland Software	
Proveedor de soporte	Giga de Colombia S.A.S.	
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)	

Atributo	Descripción	
	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 12 Ficha Técnica Visual medicas 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.	
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
	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	

Fuente: Elaboración propia SISAM

Tabla 13 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	
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

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

Tabla 14 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

Política	Descripción
	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 SaludSis

Fuente: Elaboración propia GRUGI

8.1.7. 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 15 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

Categoría	Capacidad	Cuenta con la Capacidad en la Entidad
Seguridad	Gestionar seguridad de la información	SI

Fuente: Elaboración propia GRUGI

8.1.8. Tablero de control de TI

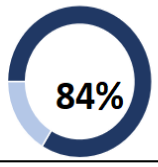
La DIGSA cuenta con un tablero de indicadores que visualiza información trimestral, lo que permite tener una visión general del avance de la estrategia TI de la entidad y del sector en la compilación de información de las variables. Se miden siete ítems, los cuales corresponden en resumen a la siguiente información:

Tabla 16 Tablero de control TI

DIGSA

TABLERO DE CONTROL PETI 2024 - 2026

INDICADOR ACUMULADO II TRIMESTRE



INDICADORES PETI								2024				
ID	TIPO DE INDICADOR	INDICADOR	%	FORMULA	VARIABLES	FRECUENCIA	RESPONSABLE	I TRIMESTRE	II TRIMESTRE	III TRIMESTRE	IV TRIMESTRE	CONSOLIDADO AÑO 2024
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	100%	100%	98%	95%	98%
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	92%	88%	90%	92%	91%
indicador 3	Operación	Cumplimiento de los ANS de proveedores	IC	IC= (SE / SP) *100)	**SE**= # de servicios planeados en periodo analizado **SE**= # de servicios ejecutados	SEMESTRAL	SISAM	0%	33%	NA	100%	66%
indicador 4	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	SEMESTRAL	SISAM	0%	99%	NA	97%	98%
indicador 5	Proyectos	Avance cronograma de proyectos	IAC	AVANCE EN CRONOGRAMA PROYECTOS **TI** DURANTE PERIODO ANALIZADO		SEMESTRAL	SISAM	0%	51%	NA	82%	82%
indicador 6	Estratégicos	Variación en trámites atendidos	PAT	AT = (TA / NT) *100	**NT**: Total de trámites que tiene la entidad **TA**: Trámites Autorizados en la entidad.	TRIMESTRAL	AFILIACIÓN	55%	44%	49%	58%	52%
indicador 7	Estratégicos	Cumplimiento presupuestal funcionamiento de TI	VTA	VTA = ((TT - TA) / TA) *100	**TT**: No. total de trámites atendidos en el actual período. **TA**: No. total de trámites atendidos en el anterior período.	TRIMESTRAL	AFILIACIÓN	100%	100%	100%	100%	100%

ID	TIPO	INDICADOR	%	FORMULA	VARIABLES	FRECUENCIA
1	Operación	Índice de disponibilidad de aplicativo WEB	ID	ID= (TSA-TB) /TSA*100)	TSA=Tiempo de servicio acordado TB= sumatorio de los tiempos sin servicio	Trimestral

2	Operación	Índice 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

3	Operación	Cumplimiento de los ANS de proveedores	IC	IC= (SE / SP) *100)	SE= # de servicios planeados en periodo analizado
					SE= # de servicios ejecutados en periodo analizado
						Semestral

ID	TIPO	INDICADOR	%	FORMULA	VARIABLES	FRECUENCIA
4	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	Semestral
6	Estratégicos	Variación en trámites atendidos	PAT	AT = (TA / NT) *100	NT: Total de trámites que tiene la entidad TA: Trámites Autorizados en la entidad.	Trimestral
7	Estratégicos	Cumplimiento presupuestal funcionamiento de TI	VTA	VTA = ((TT - TA) / TA) *100	TT: No. total de trámites atendidos en el actual período. TA: No. total de trámites atendidos en el anterior período.	Trimestral

Fuente: Elaboración propia SISAM

8.2. 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 oriente el direccionamiento y supervisión ejecutiva y además garantice el alineamiento, la planeación, organización, entrega de servicios de TI de manera oportuna, continua y segura.

8.2.1. Modelo de Gobierno de TI

8.2.1.1. 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 en el Equipo Táctico - Operativo para el Gobierno de Datos y Gobierno de Tecnologías de la Información de la Dirección General de Sanidad Militar, 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.

8.2.1.2. 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 17 Matriz de Riesgos

Referencia	Nombre del Riesgo	Clasificación del Riesgo	Plan de Acción
1	Posibilidad de Afectación Económica y Reputacional por perdida de la integridad y disponibilidad de la información debido a fallas en la infraestructura tecnológica, de comunicaciones y sistemas de información. - PROGTIC - SISAM	Seguridad de la Información	Contratación de servicios tecnológicos para el análisis de la infraestructura tecnológica de la DIGSA, que genera un informe sobre estado actual y las acciones a nivel hardware y software a realizar. Se elabora el plan de continuidad de acuerdo a los resultados dentro de la contracción, el responsable de servidores consolidara las necesidades técnicas y requerimientos a nivel de hardware y software para garantiza la infraestructura 24/7 El responsable de Seguridad de Información, revisara los controles de acceso implementados e implementara aquellos para el fortalecimiento de la mitigación del riesgos de acuerdo a los siguiente controles: Gestión de las vulnerabilidades técnicas: Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. Controles de redes: Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones. Seguridad de los servicios de red: Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente. Políticas y procedimientos de transferencia de información: Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación. Gestión de capacidad: Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura. Cadena de suministro de tecnología de información y comunicación: Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de

Referencia	Nombre del Riesgo	Clasificación del Riesgo	Plan de Acción
			seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
2	Posibilidad de Afectación Económica y Reputacional por perdida de la integridad confidencialidad de la información debido eliminación de información reservada o Publica pérdida, hurto, fuga, destrucción y/o desviación de información, por accesos no autorizados de usuarios debido a la inadecuada gestión de permisos de acceso a los sistemas de información.	Seguridad de la Información	El responsable de Seguridad de Información revisara los controles de acceso implementados e implementara aquellos para el fortalecimiento de la mitigación del riesgos, de acuerdo a los siguientes controles: Política de control de acceso: Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. Política sobre el uso de los servicios de red: Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente. Registro y cancelación del registro de usuarios: Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. Suministro de acceso de usuarios: Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios. Gestión de información de autenticación secreta de usuarios: Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal. Retiro o ajuste de los derechos de acceso: Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios. Acuerdos de confidencialidad o de no divulgación: Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
3	Posibilidad de Afectación Económica y Reputacional por perdida de la integridad, disponibilidad y confidencialidad de la	Seguridad Digital	El responsable de Seguridad de Información revisara los controles de acceso implementados e implementara aquellos para el fortalecimiento de la mitigación del riesgos, de acuerdo a los siguientes controles: Controles contra códigos maliciosos: Control: Se deberían

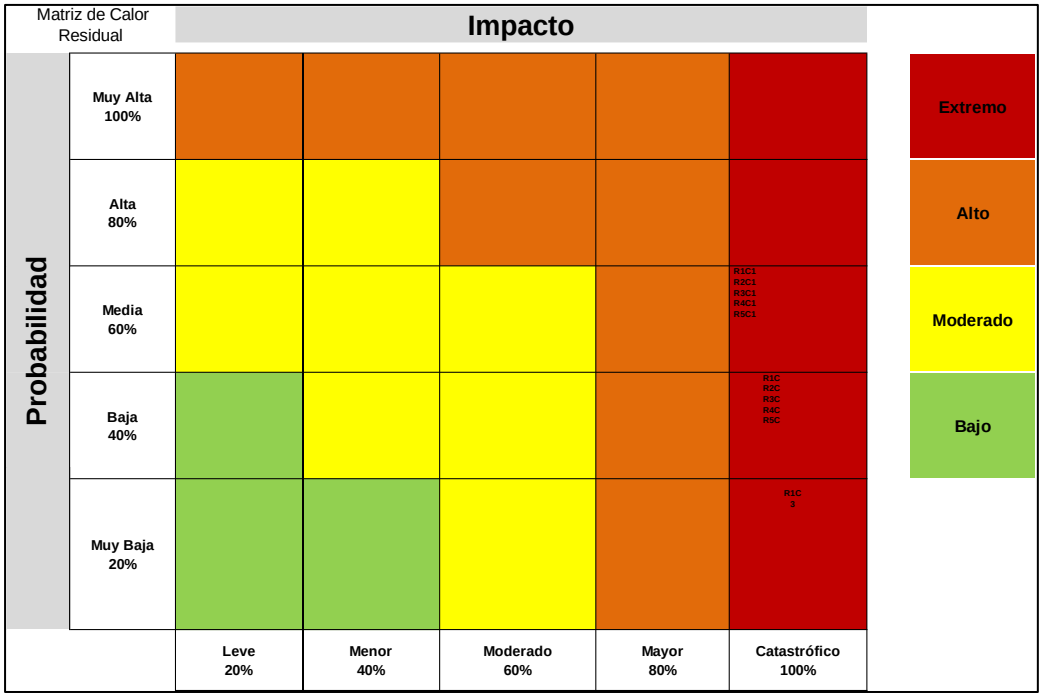
Referencia	Nombre del Riesgo	Clasificación del Riesgo	Plan de Acción
	información por la eliminación, hurto o fuga de información pública o reservada debido a ataques cibernéticos.		implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. Teletrabajo: Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo. Política sobre el uso de controles criptográficos: Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. Seguridad del cableado: Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño. Seguridad de equipos y activos fuera de las instalaciones: Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones. 0 Protección de registros: Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
4	Posibilidad de Afectación Económica y Reputacional por perdida de la integridad, disponibilidad de la información por perdida de activos de información debido a desastres o eventos fortuitos.	Seguridad de la Información	El responsable de Seguridad de Información revisara los controles de acceso implementados e implementara aquellos para el fortalecimiento de la mitigación del riesgo, de acuerdo al siguiente control: Respaldo de información: Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada. Gestión de las vulnerabilidades técnicas: Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

Referencia	Nombre del Riesgo	Clasificación del Riesgo	Plan de Acción
			Mensajería electrónica: Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
5	Posibilidad de Afectación Económica y Reputacional por perdida de la disponibilidad de la información por uso y administración no autorizada de servidores y equipos de comunicación debido a la inadecuada gestión de roles para la administración y gestión de la infraestructura tecnológica.	Seguridad de la Información	El responsable de Seguridad de Información revisara los controles de acceso implementados e implementara aquellos para el fortalecimiento de la mitigación del riesgos, de acuerdo al siguiente control: Perímetro de seguridad física: Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información. Controles físicos de entrada: Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. Política de control de acceso: Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. Sistema de gestión de contraseñas: Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas. Ubicación y protección de los equipos: Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado. Registros del administrador y del operador: Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.

Fuente: Elaboración propia SISAM

Dentro de la actualización de los Riesgos de Seguridad de la Información y ciberseguridad se debe adelantar la identificación de la infraestructura crítica y los activos de información priorizados, igualmente se tomará como referencia la Guía de Inventario y Clasificación.

Ilustración 4. Mapa de Riesgos Residuales



Fuente: Elaboración propia SISAM

8.2.1.3. 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, se presenta la gestión financiera de TI durante 2024.

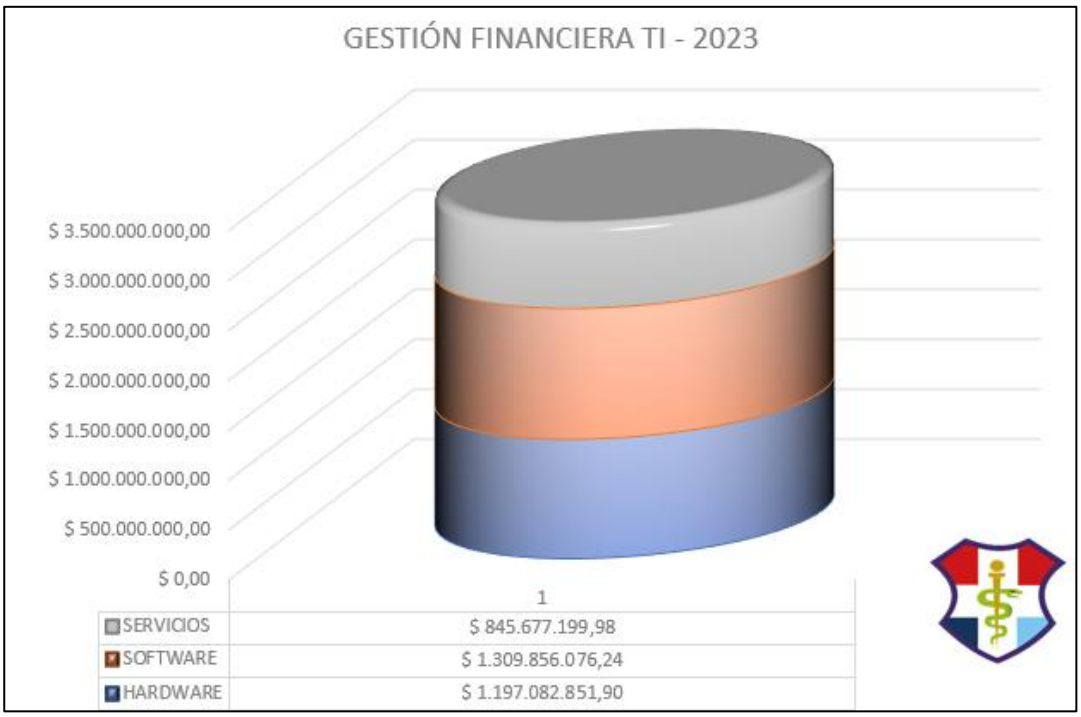


Tabla 18 Gestión financiera de TI 2023

PROCESO	VALOR HADWARE	VALOR SOFTWARE	VALOR SERVICIOS
Computadores de escritorio	$ 555.520.791,90		
Adquisición servicios de conmutador telefónico			$ 150.000.000,00
Licenciamiento soporte firewall		$ 520.213.000,00	
Licenciamiento End Point seguridad			
Solución en seguridad correo electrónico FORTIMAIL			
Servicio SOC, NOC, SOAR, SASE			$ 250.000.000,00
Canales dedicados y conexión a internet fortaleza			$ 102.357.199,98
Continuidad del negocio - servicio en la nube			$ 30.000.000,00
Licenciamiento soporte y mantenimiento - KACTUS		$ 69.029.000,00	
Licenciamiento suite adobe Acrobat		$ 9.000.000,00	
Licenciamiento Office 365		$ 711.614.076,24	
Licenciamiento sistema operativo DATACENTER			

PROCESO	VALOR HADWARE	VALOR SOFTWARE	VALOR SERVICIOS
Licenciamiento Win Server CAL			
Extensión garantías de servidores			$ 63.320.000,00
Switches Acces Point	$ 600.000.000,00		
Página web - Hosting			$ 250.000.000,00
Pantallas interactivas	$ 37.473.100,00		
Transcever y conectores telefónicos	$ 4.088.960,00		
TOTAL	**$ 1.197.082.851,90**	**$ 1.309.856.076,24**	**$ 845.677.199,98**

Fuente: Elaboración propia SISAM

8.2.1.4. Gestión de asignación de Recursos Humanos

Aunque durante el 2022 se realizó incorporación a la planta de personal de los funcionarios de carrera administrativa, no se logró reclutar personal con el perfil necesitado para la oficina de tecnologías de la información el cual se encuentra conformado así:

Tabla 19 Recurso Humano SISAM -SALUS SIS

Área	Profesión	Apellidos y Nombre	Rol
Grupo Sistema Integral De Información – Tecnologías De La Información Y Las Comunicaciones - SISAM	Oficinal de Apoyo Administrativo	TC. Elizabeth Bocarejo Bautista	Coordinadora
	Ingeniero de Sistemas	OPS. Ramiro Lozano Arboleda	Asesor
Área Infraestructura, Redes Y Comunicaciones - ARECO	Sub Oficinal de Apoyo Administrativo	SS. Andrés Felipe Perdomo Franco	Líder
	Ingeniero de Sistemas	PD. Yeison Antonio Yara Guevara	Apoyo
	Tecnóloga Ambiental	TASD. Maryori Tatiana Leiva Ubillus	Apoyo
	Administradora de Empresa	TASD. Yamile López	Apoyo
	Administrador Publico	TASD. Cristian Camilo Rodríguez Delgado	Apoyo
	Ingeniero de Sistemas	TASD. Gustavo Adolfo Torres Forero	Apoyo

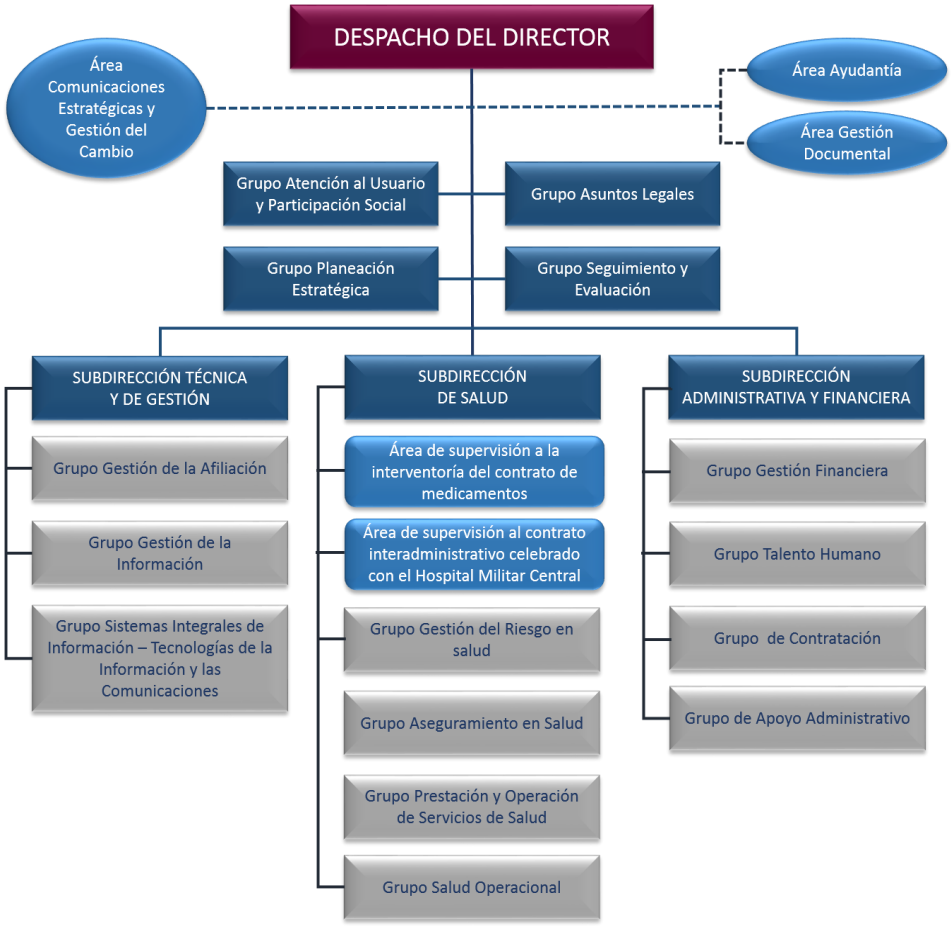
Área	Profesión	Apellidos y Nombre	Rol
	Tecnóloga en Gestión de Redes de Datos	AASD. Linda Jasbleidy Rodríguez Vásquez	Apoyo
Área Seguridad De La Información	Sub Oficinal de Apoyo Administrativo	S1. Deisy Milena Zarate Martínez	Líder
	Ingeniero de Sistemas	PD. Roberto Rodríguez Perdomo	Apoyo
	Ingeniero de Sistemas	PS. Víctor Hugo Navarro Cierra	Apoyo
Área Administración Del Sistema Y Base De Datos	Oficinal de Apoyo Administrativo	TC. Jorge Darwin Guevara Guerrero	Líder
	Ingeniero de Sistemas	PD. Julio Cesar Salgado Guerrero	Apoyo
	Ingeniero de Sistemas	PD. Juan Orlando Ramos Valbuena	Apoyo
	Ingeniero Electrónico - Especialista Power BI	PS. Néstor Andrés Gómez	Apoyo
Sistema De Información SaludSis	Oficinal de Apoyo Administrativo	CR. José Mauricio Barrera Barrera	Gerente de proyecto SALUD.SIS
	Enfermera Jefe	PS. Ingrid Mileyda Martínez Guevara	Apoyo
	Auxiliar de Enfermería	PS. Karen Vanessa Maestre Mercado	Apoyo

Fuente: Elaboración propia SISAM

8.2.2. 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 5.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 6.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 7.Gobierno Digital SISAM

8.2.3. Gestión de Proyectos de TI

Dentro de la revisión del Proceso de Gestión de Proyectos TI no se evidencia la implementación del Modelo de Gestión de Proyectos TI – MGPTI del Marco de Arquitectura Empresarial, sin embargo, el Grupo de Sistemas Integral de Información – Tecnologías de la Información y las Comunicaciones – SISAM incorpora para su gestión algunos lineamientos que se enmarcan en esta metodología, a continuación, se presenta los aspectos implementados de cada uno de los dominios:

8.2.3.1. Dominio Legal

El Grupo de Sistemas Integral de Información – Tecnologías de la Información y las Comunicaciones – SISAM, estructuran los proyectos TI acorde a los lineamientos normativos tanto a nivel misional, operacional, estratégico y de apoyo dentro del marco de la misionalidad.

8.2.3.2. Dominio de Planeación

- Análisis del Contexto Interno y Externo.
- Identificación de Proyecciones tecnológicas.
- Identificación de necesidades y brechas tecnológicas con los Grupos Internos de Trabajo.
- Formulación de Proyectos Tecnológicos Viabilizados en el Comité Institucional de Gestión y Desempeño alineados al Plan Estratégico Sectorial, Plan Estratégico Institucional.
- Presentación y Viabilizados en el Comité de Integración de Tecnologías de Información CITI.

8.2.3.3. Dominio de Ejecución

- Asignación Supervisión del Contrato teniendo en cuenta el Perfil Técnico
- Mesas de Trabajo Proveedores, Supervisor, Gerente Proyecto
- Informes de Mensuales de Supervisión
- Revisión Plan de Trabajo

8.2.3.4. Dominio de Control

- Pruebas de Desarrollo por parte de los Funcionales y Contratista para proyectos de Desarrollo Tecnológico.
- Evaluación de Criterios de Usabilidad y Accesibilidad Sistema de Información.
- Análisis de Riesgos dentro del Proceso de Ejecución.
- Análisis de vulnerabilidades
- Pruebas de recuperación

Con lo anterior, como acciones de mejora se debe realizar la implementación de los dominios que incorpora el Modelo de Gestión de Proyectos TI – MGPTI del Marco de Arquitectura Empresarial en sus Cuatro Dominios (Contexto Estratégico, Planeación, Ejecución y Control y Cierre y Operación), para lo cual se deberá realizar un autodiagnóstico que permita establecer las actividades priorizadas y proyectadas a desarrollar dentro de la vigencia del Presente Plan.

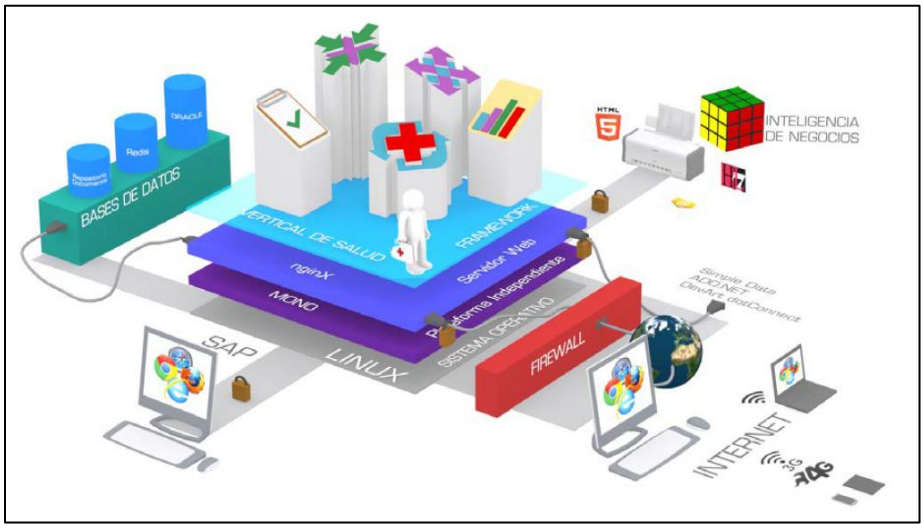
8.3. Gestión de Información

8.3.1. 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 8. Modelo de Gestión de la Información SALUD.SIS



Fuente: Elaboración propia SISAM

8.3.2. 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.

8.3.3. 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 liderada por el Grupo de Gestión de la Información – GRUGI, Área Estandarización de Datos y Formatos – ARAFO, con el apoyo del área de Planeación Estratégica (GRUPL), pero la responsabilidad de la información es transversal.

- 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).

8.4. 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.

8.4.1. 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 20 Catalogo de SI

Atributo	Descripción
Nombre del Sistema	Sistema De Gestión De Documento Electrónico De Archivo
Sigla	SGDEA
Descripción de Sistema	Sistema de Gestión Documental Electrónico de Archivo para el Comando General de las Fuerzas Militares
Versión	1.0
Categoría	Sistema de Apoyo
Tipo de Desarrollo	Software como Servicio
Fabricante	IOIP S.A.S.
Proveedor de Soporte	IOIP S.A.S.
Fecha de Vencimiento del soporte	1/12/2022
Responsable Técnico	CGFM
Responsable Funcional	CGFM
Estado	Activo
Licenciamiento	N/A
Sistema Operativo	N/A
Lenguaje de Programación	.NET
Documentación Técnica y funcional	En el menú de sistema en la pestaña **ayuda** se encuentra Manual de Usuario, Videos tutoriales.
Observaciones	

Atributo	Descripción
Nombre del Sistema	Sistema de Administración del Talento Humano (KACTUS)
Sigla	KACTUS
Descripción de Sistema	Sistema de recursos humanos y nómina KACTUS-HR
Versión	20.0.0.0
Categoría	Sistema de Apoyo
Tipo de Desarrollo	Software como Servicio

Atributo	Descripción
Fabricante	DIGITALWARE
Proveedor de Soporte	DIGITALWARE
Fecha de Vencimiento del soporte	31/12/2024
Responsable Técnico	Supervisor técnico
Responsable Funcional	Supervisor funcional
Estado	Activo
Licenciamiento	1 licencia perpetua con acceso a nuevas versiones anualmente por contrato
Sistema Operativo	Windows
Lenguaje de Programación	Delphi
Documentación Técnica y funcional	Si, carpeta compartida
Observaciones	Tanto la base de datos como el aplicativo se encuentran instalados en centro de datos DIGSA.

Atributo	Descripción
Nombre del Sistema	Sistema de Administración del Talento Humano (KACTUS)
Sigla	KACTUS
Descripción de Sistema	Sistema de recursos humanos y nómina KACTUS-OPHELIA
Versión	20.0.0.0
Categoría	Sistema de Apoyo
Tipo de Desarrollo	Software como Servicio
Fabricante	DIGITALWARE
Proveedor de Soporte	DIGITALWARE
Fecha de Vencimiento del soporte	31/12/2024
Responsable Técnico	Supervisor técnico - SISAM
Responsable Funcional	Supervisor funcional
Estado	Activo
Licenciamiento	1 licencia perpetua con acceso a nuevas versiones anualmente por contrato
Sistema Operativo	Windows
Lenguaje de Programación	Delphi
Documentación Técnica y funcional	Si
Observaciones	Tanto la base de datos como el aplicativo se encuentran instalados en centro de datos DIGSA.

Atributo	Descripción
Nombre del Sistema	Sistema de Gestión Documental (ONBASE)
Sigla	ONBASE
Descripción de Sistema	Sistema de gestión documental que ayuda en la administración y organización de la documentación de los procesos
Versión	21
Categoría	Sistema de Apoyo
Tipo de Desarrollo	Software como Servicio

Atributo	Descripción
Fabricante	HYLAND
Proveedor de Soporte	GIGA SAS
Fecha de Vencimiento del soporte	1/12/2024
Responsable Técnico	Supervisor técnico
Responsable Funcional	Supervisor funcional
Estado	Inactivo
Licenciamiento	1 licencia perpetua con acceso a nuevas versiones anualmente por contrato
Sistema Operativo	Windows
Lenguaje de Programación	Sin información
Documentación Técnica y funcional	Si, carpeta compartida
Observaciones	Tanto la base de datos como el aplicativo se encuentran instalados en centro de datos propio.

Atributo	Descripción
Nombre del Sistema	ERP-SAP
Sigla	SAP
Descripción de Sistema	Sistema de administración de recursos financieros
Versión	6.0.6
Categoría	Sistema de Apoyo
Tipo de Desarrollo	Software como Servicio
Fabricante	SAP SE
Proveedor de Soporte	SAP COLOMBIA MEDIANTE EL SILOG
Fecha de Vencimiento del soporte	1/12/2024
Responsable Técnico	SILOG-MDN
Responsable Funcional	SILOG-MDN
Estado	Activo
Licenciamiento	960 licencias perpetuas con acceso a nuevas versiones anualmente por contrato
Sistema Operativo	Windows
Lenguaje de Programación	ABAP
Documentación Técnica y funcional	No
Observaciones	Se encuentra instalado en el Ministerio de Defensa bajo la administración del SILOG.

Atributo	Descripción
Nombre del Sistema	Sistema integral de información del SSFM
Sigla	SALUD.SIS
Descripción de Sistema	Sistema integral de información del SSFM
Versión	9.6.6.2
Categoría	Sistema Misional
Tipo de Desarrollo	Desarrollo a la medida
Fabricante	DIGSA
Proveedor de Soporte	GROWDATA
Fecha de Vencimiento del soporte	14/04/2024

Atributo	Descripción
Responsable Técnico	Gerente del Proyecto
Responsable Funcional	Subdirección de Salud
Estado	Activo
Licenciamiento	Oracle
Sistema Operativo	Windows
Lenguaje de Programación	.NET
Documentación Técnica y funcional	https://portal.saludsis.mil.co/Account/DescargarManualDeUsuario
Observaciones	Tanto la base de datos como el aplicativo de producción se encuentran instalados en centro de datos del Ministerio de Defensa Nacional – Fortaleza.

Atributo	Descripción
Nombre del Sistema	SUITE VISION EMPRESARIAL
Sigla	SUITE VISION
Descripción de Sistema	Software de Gestión de Portafolio de Proyectos
Versión	9.6.62-20230428
Categoría	Sistema de Apoyo
Tipo de Desarrollo	Software como Servicio
Fabricante	PENSEMOS
Proveedor de Soporte	PENSEMOS POR MEDIO DEL CGFM
Fecha de Vencimiento del soporte	N/A
Responsable Técnico	CGFM
Responsable Funcional	Grupo de Planeación de la DGSM
Estado	Activo
Licenciamiento	N/A
Sistema Operativo	Windows
Lenguaje de Programación	Sin Información
Documentación Técnica y funcional	Manual en Línea Portal Institucional
Observaciones	Se opera bajo ambiente WEB, bajo la administración del CGFM.

Atributo	Descripción
Nombre del Sistema	Sistema Integral de Información Financiera
Sigla	SIIF
Descripción de Sistema	Herramienta modular automatizada que integra y estandariza el registro de la gestión financiera pública, con el fin de propiciar una mayor eficiencia en el uso de los recursos de la Nación y de sus entidades descentralizadas, y de brindar información oportuna y confiable.
Versión	2024
Categoría	Sistema de Apoyo
Tipo de Desarrollo	Desarrollo Externo
Fabricante	Ministerio de Hacienda - MINHACIENDA
Proveedor de Soporte	MINHACIENDA

Atributo	Descripción
Fecha de Vencimiento del soporte	MINHACIENDA
Responsable Técnico	MINHACIENDA
Responsable Funcional	MINHACIENDA
Estado	Activo
Licenciamiento	MINHACIENDA
Sistema Operativo	Windows
Lenguaje de Programación	N/A
Documentación Técnica y funcional	Manual en Línea Pagina Institucional
Observaciones	Sistema de información administrado por el Ministerio de Hacienda y Crédito Público.

Fuente: Elaboración propia SISAM

8.4.2. Capacidades Funcionales de los Sistemas de Información

Para el cumplimiento de los objetivos de los 19 procesos que conforman el Mapa de Procesos Institucional, se dispone de Sistemas de Información que apoyan la gestión de las tareas y/o actividades, en la siguiente matriz se relaciona las capacidades funcionales de cada una de estas aplicaciones.

Tabla 21 Capacidades Funcionales de los Sistemas de Información

Función	PORTAL SIS	KACTUS	PAGINA WEB	ERP - SAP	SUITE VISION	Visual Medica	OnBase	SIIF	SGDA	SECOP	BIZAGI	PIIP
Administración de Recursos Financieros		X		X				X				
Administración del Talento Humano		X										
Apoyo Sistema de Gestión					X							
Certificaciones Laborales		X	X									
Certificados Laborales		X	X									
Desprendibles de Pago		X	X									
Flujo de Información					X							
Gestión de Costos				X								
Gestión de Afiliación y tramites en Salud (Registro de Afiliación, Actualización de Datos, Agendamientos de Citas, Encuestas de Satisfacción, Historia Clínica, Autorizaciones, Cuentas Medicas)	X											
Gestión de Contratación										X		
Gestión de Documentos Electrónicos									X			
Gestión de Riesgos					X							
Gestión de Tramites y Servicios			X									
Gestión Financiera Publica							X					
Gestión PQRSD con los Ciudadanos	X		X									
Gestión Presupuestal								X				

Función	PORTAL SIS	KACTUS	PAGINA WEB	ERP - SAP	SUITE VISION	Visual Medica	OnBase	SIIF	SGDA	SECOP	BIZAGI	PIIP
Hoja de Vida Funcionarios		X					X					
Liquidación de Nomina		X										
Radicación de Comunicaciones Externa									X			
Radicación de Comunicaciones Internas									X			
Trámites administrativos - BIZAGI											X	
Trámites Inversión Publica												X
Visualización, informes y distribución de Estudios Radiológicos						X						

Fuente: Elaboración propia SISAM

8.4.3. Mapa de Integraciones objetivo de sistemas de Información

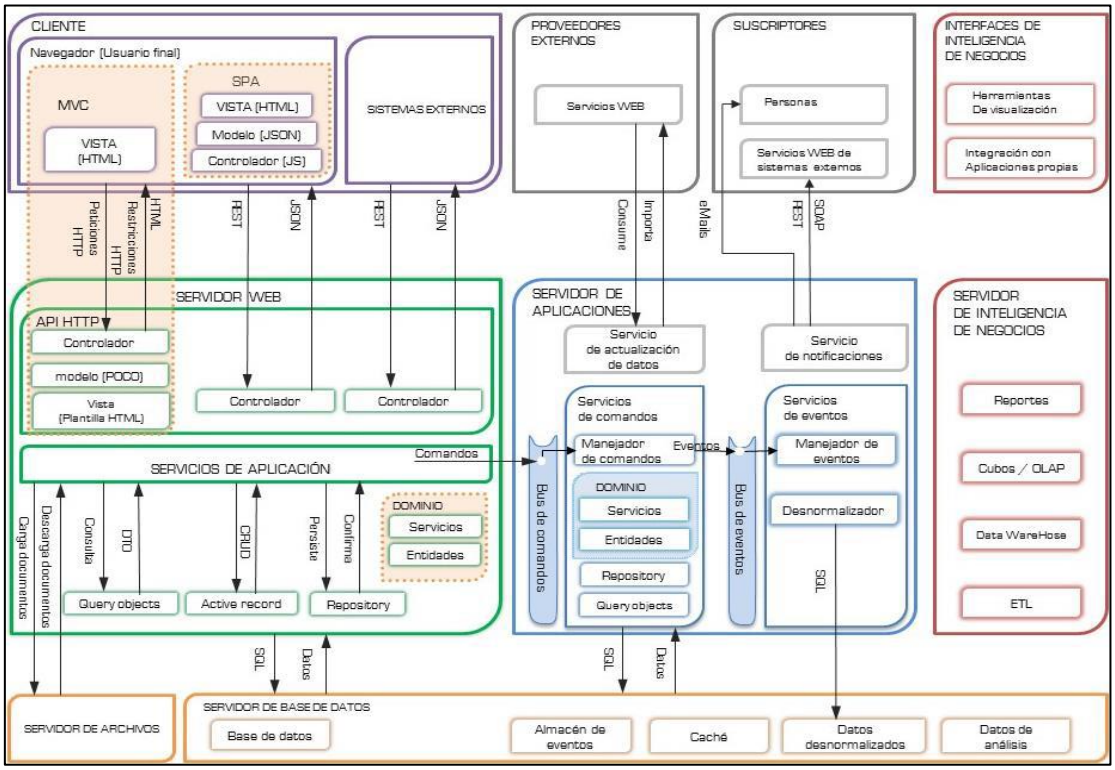
Sistemas de Información	Propósito	Protocolo de Integración	Esquema de Seguridad
Portal SALUD.SIS	Gestión de Afiliación y tramites en Salud (Registro de Afiliación, Actualización de Datos, Agendamientos de Citas, Encuestas de Satisfacción, Historia Clínica, Autorizaciones, Cuentas Medicas)		

Fuente: Elaboración propia SISAM

8.4.4. Arquitectura de Referencia de Sistema de Información.

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:

Ilustración 9.Integración de la aplicación SaludSIS



Fuente: CDR CODALTEC

8.4.5. Ciclo de Vida de los Sistemas de Información

Tabla 22 Ciclo de vida de los sistemas de información

Actividad	Grado de Madurez (Optimizado, Implementado Informal, No tiene, No aplica	Descripción del Hallazgo u Oportunidad de Mejora
Levantamiento de Necesidades de Sistemas de Información	Implementado Para cambios en el Sistema Información SALUD.SIS se tiene implementado el formato de solicitud de requerimientos donde se establecen los criterios de solicitud, propuesta y validación, Prioridad, Descripción de la Solicitud (Requerimiento, Para que, Dado Que, Cuando, Entonces y Evidencias, Anexos).	Los líderes funcionales tengan el contexto generalizado de las solicitud, propuestas y validación del requerimiento. Que existe un funcionario Operativo de SALUD.SIS y no depender de un Contrato.
Análisis de requisitos funcionales y no funcionales	Implementado Validación en conjunto con el Gerente del Proyecto, Enlace Funcional, el Funcional y el Equipo de Soporte, de la	Establecer un Procedimiento y/o lineamientos que permita estructurar equipo Táctico, Operativo - Funcional.

Actividad	Grado de Madurez (Optimizado, Implementado Informal, No tiene, No aplica	Descripción del Hallazgo u Oportunidad de Mejora
	Solicitud, Propuesta y Validación requerido en el Formato Solicitud de Requerimiento SALUD.SIS y Tecnologías de la Información. Aprobada la validación de la propuesta se realizada comunicación con enlace funcional, Gerente del Proyecto, supervisor del contrato para inicio del Diseño de la Solución.	Emitir lineamientos para definir el esquema de control y seguimiento en las actividades de soporte, mantenimiento y evolución del sistema de información
Diseño de la solución	Implementado Se realiza refinamiento de la Historia de Usuarios. Mesas de Trabajo con los Funcionales, enlace funcional, gerente de proyecto, transversales al requerimiento para levantamiento de Historia de Usuarios.	Ajustar formato de requerimiento Formato Solicitud de Requerimiento SALUD.SIS y Tecnologías de la Información incorporando Análisis de Impacto/Urgencia y Matriz de Riesgos, implementar formato plan de pruebas.
Codificación del software	Implementado Proveedor (Contratista) inicia desarrollo de acuerdo con la solicitud de requerimiento con la propuesta y validación. Mesas de trabajo Gerente del Proyecto, Enlace Funcional, el Funcional y el Equipo de Soporte, cuando se presenten observaciones.	
Aseguramiento de la calidad (pruebas)	Utilización de Ambiente de Pruebas, funcional, equipo de soporte, Gerente de Proyecto y Proveedores. Utilización de Ambiente de preproducción validado por el funcional, enlace funcional y Gerente de Proyecto, para despliegue de producción.	Ajustar formato de requerimiento Formato Solicitud de Requerimiento SALUD.SIS y Tecnologías de la Información alineado al formato de pruebas del Sistemas de Información.
Despliegue en Producción	Programación de Ventana de Mantenimiento de acuerdo con el impacto de usuarios y requerimiento.	Ajustar formato de requerimiento Formato Solicitud de Requerimiento SALUD.SIS y Tecnologías de la Información, incorporando Plan de Ejecución y Plan de Reversión (Roll-Back).

Fuente: Información propia SISAM

8.4.6. 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.

8.4.7. Mantenimiento de los Sistemas de información

Tabla 23 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 - Hacer el diseño y desarrollo de la solución

Actividad	Grado de madurez	Descripción hallazgo u oportunidad de mejora
		- 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

8.4.8. Mantenimiento de los Sistemas de información

Tabla 24 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

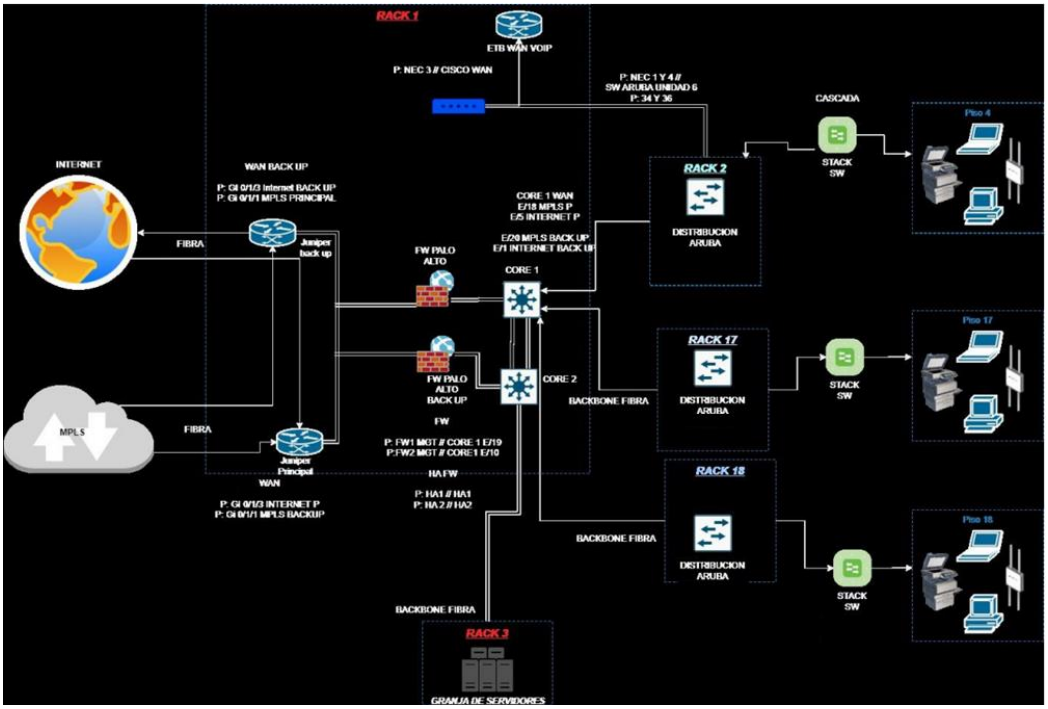
8.5. Infraestructura de TI

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).

La topología de red consiste en una red central ubicada en las oficinas principales, esta actúa como punto de concentración para LAN remotas (Oficinas Externas) y la Nube de Oracle-Fortaleza. Las LAN están conectadas a la red central a través de enlaces WAN dedicados MPLS y VPN Site To Site. Por medio del CORE y de los equipos perimetrales de seguridad, los diferentes sitios se interconectan debido a las rutas estáticas y políticas presentes. La seguridad de la red está basada mediante firewalls.

Ilustración 10.Topología de red



Fuente: Información propia SISAM

8.5.1. Arquitectura de Infraestructura tecnológica

Tabla 25. Catálogo de Servicios de Infraestructura de TI

ID Servicios de Infraestructura	Servicio de Infraestructura	Descripción
ST.SI.01	Nube	• Servicio de directorio activo que almacena información acerca de los objetos de una red y facilita su búsqueda y uso por parte de los usuarios y administradores. • Office 365 Plataforma Proporciona herramientas y software para la creación, edición, almacenamiento y colaboración en documentos, hojas de cálculo y presentaciones, facilitando tareas administrativas y de productividad dentro de la entidad.
ST.SI.02	Seguridad	• Herramientas Firewall, Antivirus XDR Cortex y FortiMail para Monitorización y Detección: supervisar redes, correo y sistemas. • Centro de operaciones de red (NOC) • Centro de operaciones de seguridad (SOC) • (VICARIUS VRX) que hace análisis de vulnerabilidades y permite remediar en tiempo real con agentes instalados en cada Endpoint, servidor o infraestructura tecnológica instalada con una plataforma centralizada independiente por cada grupo de activos.

ID Servicios de Infraestructura	Servicio de Infraestructura	Descripción
ST.SI.03	Telefonía IP	• Permite realizar llamadas de voz a través de internet utilizando el protocolo IP (Internet Protocol), brindando una opción moderna y eficiente a la telefonía habitual.
ST.SI.04	Almacenamiento	• Oracle Database Appliance (ODA) es una de las diversas tecnologías de servidor que Oracle ha desarrollado y personalizado para su uso en su propia base de datos Oracle DB. • Sistema NAS almacenamiento de alta capacidad conectado a una red que permite a los usuarios y clientes autorizados almacenar y recuperar datos en una ubicación centralizada.
ST.SI.05	Servidores	• Servicio de infraestructura de hardware para el alojamiento de aplicaciones y Base de Datos.
ST.SI.06	Mesa de Servicios	• Herramienta de Servicios Zendesk para la gestión de solicitudes de incidentes y requerimientos de tecnología. • Acuerdos de Nivel de Servicios mediante la herramienta mesa de ayuda.
ST.SI.07	Periféricos	• Servicios asociados a los equipos asignados a los usuarios finales como son computadoras e impresoras.
ST.SI.08	Redes	• Servicios LAN Dirección General de Sanidad Militar y Servicio WAN Ministerio de Defensa.

Fuente: Elaboración propia SISAM

8.5.2. 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 26 Capacidad de la Infraestructura Tecnológica

Nombre de Dispositivo	Proveedor	Número dispositivos	Soporte IPV6
Microsoft Virtual WiFi Miniport Adapter	Microsoft	142	N/A
Realtek PCIe GBE Family Controller	Realtek	98	SI
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
Intel(R) Ethernet Connection I217-V	Intel Corporation	59	SI
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

Nombre de Dispositivo	Proveedor	Número dispositivos	Soporte IPV6
Intel(R) Dual Band Wireless-AC 3165	Intel Corporation	39	SI
Intel(R) Ethernet Connection (5) 1219-LM	Intel	39	SI
Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Client)	Broadcom Corporation	16	SI
HP NC553i Dual Port Flex Fabric 10Gb Converged Network Adapter	Emulex	16	SI
Intel(R) 82567LM-3 Gigabit Network Connection	Intel	13	SI
Conexi6n de red Gigabit Intel(R) 82567LM-3	Intel	12	SI
Intel(R) Dual Band Wireless-AC 8260	Intel	12	SI
Intel(R) Ethernet Connection I219-LM	Intel	12	SI
Gigabit Ethernet Broadcom	Broadcom	9	SI
HP NC382i DP Multifunction	Hewlett- Packard Company	8	SI
Gigabit Server Adapter	Company		
HP NC553i Dual Port Flex Fabric 10Gb Converged Network Adapter	ServerEngines Corporation	8	SI
Broadcom BCM943228Z	Broadcom	7	SI
Intel(R) Ethernet Connection (2) 1219- LM	Intel	7	SI
Intel(R) 82574L Gigabit Network Connection	Intel Corporation	5	SI
TAP-Windows Provider V9	TAP-Windows Provider V9	5	N/A
Broadcom BCM5708C	Broadcom Corporation	4	SI
Conexi6n de red Gigabit Intel(R) V82574L	Intel Corporation	4	SI
	Broadcom Corporation	4	SI
Qualcomm Atheros QCA9565 802.llb/g/ n WiFi Adapter	Qualcomm Atheros Communication	4	SI
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
HP Network Teaming Virtual Miniport Driver	Hewlett- Packard Company	2	N/A

Nombre de Dispositivo	Proveedor	Número dispositivos	Soporte IPV6
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
lntel(R) Centrino(R) Wireless-N 2230	Intel Corporation	1	SI
Intel(R) Ethernet Connection I217-V	Intel Corporation	1	SI
Microsoft Wi-Fi	Microsoft	1	N/A
Direct Virtual ADAPTER WLAN	Broadcom	1	SI
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 PCle 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 27 Comunicaciones de TI

Marca	Descripción	Dual Stack	Dual Stack IPV6
Palo Alto PA 3220	Firewall	SI	SI
ARUBA 2930 F	SWITCH CORE	SI	SI
3COM 5500 G	SWITCH	SI	SI
HP 2920	SWITCH	SI	SI
CISCO800	SWITCH	SI	SI
HP 2920	SWITCH	SI	SI
HP 2920	SWITCH	SI	SI
HP 2920	SWITCH	SI	SI

Marca	Descripción	Dual Stack	Dual Stack IPV6
HP 2920	SWITCH	SI	SI
HP 2920	SWITCH	SI	SI
ARUBA 2930F	SWITCH	SI	SI
HP 2920	SWITCH	SI	SI
HP 2920	SWITCH	SI	SI
HP 2920	SWITCH	SI	SI
HP 2920	SWITCH	SI	SI
ARUBA 2930F	SWITCH	SI	SI
HP 2920	SWITCH	SI	SI
HP 2920	SWITCH	SI	SI
HP 2920	SWITCH	SI	SI
HP 2920	SWITCH	SI	SI
ARUBA 2930F	SWITCH	SI	SI

Fuente: Información propia SISAM

8.5.3. Administración de la Operación

El Grupo Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones, mediante sus servicios de información y Soporte a través del proceso de servicios de información y soporte tecnológico busca garantizar la disponibilidad y continuidad de los servicios tecnológicos mediante el monitoreo, análisis de capacidad tecnológica y eficiencia en la gestión de incidentes tecnológicos.

Tabla 28 Administración de operación

Identificador	Descripción	Si	No
Monitoreo de la infraestructura de TI	La entidad cuenta implementación de herramientas de SOC y NOC	X	
Capacidad de la infraestructura tecnológica	Se realiza inventario Capacidades, Obsolescencia y se incluye en Plan de Anual Compras.	X	
Gestión de Vulnerabilidades	La entidad cuenta implementación de herramientas de SOC y NOC	X	
Gestión de Requerimiento Técnicos	Se Implementa a través de la herramienta en desarrollo Power Apps	X	
Mantenimiento Preventivo y Correctivo	Se realiza inventario y se incluye en Plan de Anual Compras.	X	
Gestión Sistema de Información	Se realiza inventario y se incluye en Plan de Anual Compras.	X	
Gestión de Licenciamientos Suit de Oficina, Sistema de Información	Se realiza inventario y se incluye en Plan de Anual Compras.	X	
Disposición de Residuos Tecnológicos	No se tiene procedimiento o guía para la gestión de residuos tecnológicos.		X

Fuente: Elaboración propia SISAM

Tabla 29 Comunica Matriz de Mantenimiento

Identificador	Descripción	Si	No
Acuerdo Nivel de Servicios	No se cuenta con acuerdos de servicios		X
Mesa de Servicios	Herramienta en desarrollo Power Apps registro y monitoreo de casos soporte técnico.	X	

Identificador	Descripción	Si	No
	Herramienta Zendesk para soporte sistema de información Salud.SIS		
Planes de Mantenimiento	No se cuenta con planes de mantenimiento preventivo, a nivel correctivo se realizan actividades a demanda.		X

Fuente: Elaboración propia SISAM

8.5.4. Fases de implementación IPV&

Tabla 30 Fases de Implementación IPV6

Identificador	Descripción	Si	No
Fase de Diagnostico	La Dirección General de Sanidad Militar adquirido ante LACNIC el bloque de direcciones IPV6, por lo anterior autorizo a TIGO, para que transportara las direcciones a través de su red y fueran publicadas a sus proveedores internacionales. Igualmente, la entidad dentro de este proceso con LACNIC no adquirió el sistema autónomo (ASN) por lo tanto, la DIGSA autorizo a TIGO, para que publicara el ASN de TIGO.	X	
Fase de Implementación	La Dirección General de Sanidad Militar enruto en su firewall el bloque de direcciones IPV6.	X	
Fase de Pruebas	La Dirección General de Sanidad, realizo pruebas en varios equipos de escritorio la habilitación de IPV6, las cuales fueron positivas.	X	

Fuente: Elaboración propia SISAM

La Entidad finalizo el contrato con el proveedor de TIGO, e inicio un nuevo contrato con el proveedor de Media Commerce, por lo cual se retomó con este operador la implementación de este protocolo, y se encuentra en la fase de implementación.

8.6. Uso y 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

8.6.1. Estrategia de Uso y Apropiación

8.6.1.1. Caracterización de Grupos de Interés

Atributo	Descripción
Grupo de Interés	Funcionarios DIGSA
Descripción	Equipo de colaboradores de los diferentes procesos que conforman los Grupos Internos de Trabajo

Atributo	Descripción
Objetivo	Apoyar los procesos misionales, apoyo, estratégicos, Seguimiento y Evaluación, que permita el cumplimiento de misión, visión institucional y los objetivos estratégicos.
Rol de Involucrado	Coordinadores de Área, Lideres, Responsables de Procesos, Colaboradores de área.

Fuente: Elaboración propia SISAM

8.6.1.2. Formación y Capacitación

Tabla 31 Formación y Capacitación

ID	Temática	Nombre	Objetivo	Duración	Grupo de Impacto
1.	Herramientas Ofimáticas	Uso de la Herramienta SharePoint de office 365.	Capacitar a usuarios básicos e intermedios de la Dirección General de Sanidad Militar en el Uso de la Herramienta SharePoint de office 365	40 horas	Coordinadores de Área Subdirectores Líderes de Área Colaboradores de Área
2.	Herramientas Tecnológicas	Uso de office 365 en la pantalla interactiva adquirida para la sala Aristóteles.	Realizar capacitación a los funcionarios de la DIGSA que deseen participar, en el uso de office 365 en la pantalla interactiva adquirida para la sala Aristóteles.	10 horas	Coordinadores de Área Subdirectores
3.	Herramientas Tecnológicas	Forms y Power Automate	Realizar una charla informativa a los funcionarios de la DIGSA que deseen participar, en office 365 en los temas relacionados a: Forms y Power Automate	8 horas	Coordinadores de Área Subdirectores Líderes de Área Colaboradores de Área
4.	Tecnologías Emergentes	Transformación Digital Industria 4.0	Capacitar a los servidores públicos para aplicar los fundamentos de la industria 4.0 de la Cuarta Revolución Industrial y de la trasformación digital en el sector público	10 horas	Coordinadores de Área Subdirectores Líderes de Área Colaboradores de Área

Fuente: Elaboración propia SISAM

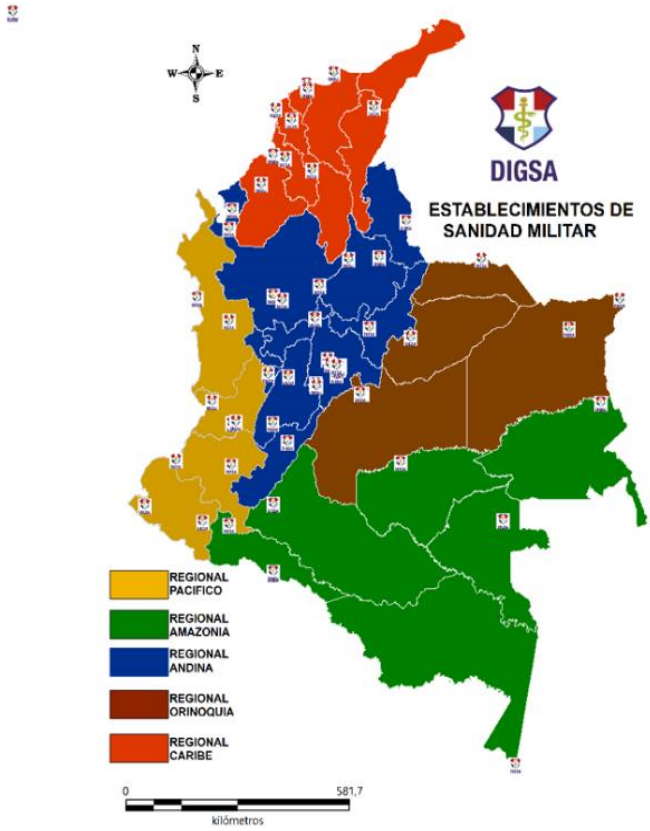
Con lo anterior se evidencia que dentro del Plan de Formación y Capacitación no existe implementados lineamientos dentro de la política de gestión del conocimiento y formación en la actualización de avances, tendencias tecnológicas, ciberseguridad e innovación que faciliten el fortalecimiento de habilidades tecnológicas, dentro de las acciones a realizar, se incluirá en Plan de Capacitaciones formación Técnico – Profesional que permita el fortalecimiento de competencias y habilidades que apoyen el cumplimiento del proceso y la misionalidad institucional.

8.6.2. Caracterización de los Grupos de Interés

Ilustración 11. Módulos de Salud.SIS

Fuente: Elaboración propia SISAM

Ilustración 12.Mapa Georreferenciado de ESM

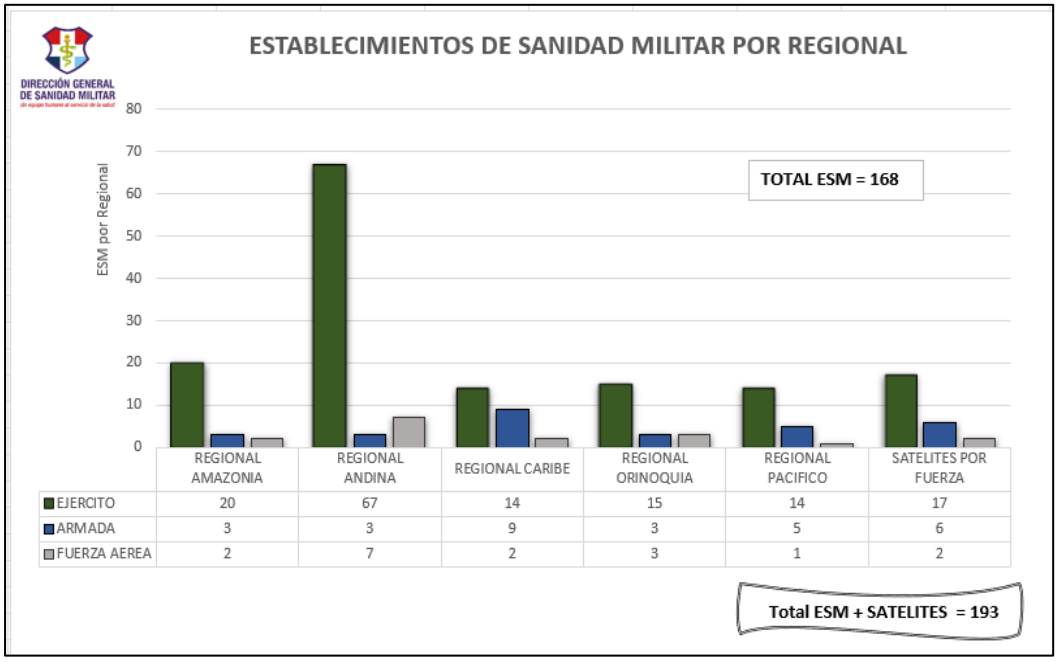


Bajo el radicado No.012007744702 del 5 julio del 2024, lineamientos para la tipificación de los establecimientos de sanidad militar del SSFM, se adjunta mapa georreferenciado con la ubicación de ESM general con todas las fuerzas, se adjunta gráfico con la lista tabular de los ESM por regional y fuerza, igualmente las unidades de apoyo a la salud operacional-Satélites.

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

Fuente: Elaboración propia GRUGI

Ilustración 13. Establecimientos de Sanidad Militar



Fuente: GRUGI Noviembre 2024

8.7. Seguridad

Teniendo en cuenta la aplicación de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información de la Política de Gobierno Digital, dentro de los dominios establecidos en la norma 27001:2013 el nivel de cumplimiento en la implementación de controles se encuentra en 58, lo cual implica la revisión en cada uno de los dominios en los criterios de medición, monitoreo y mejora continua.

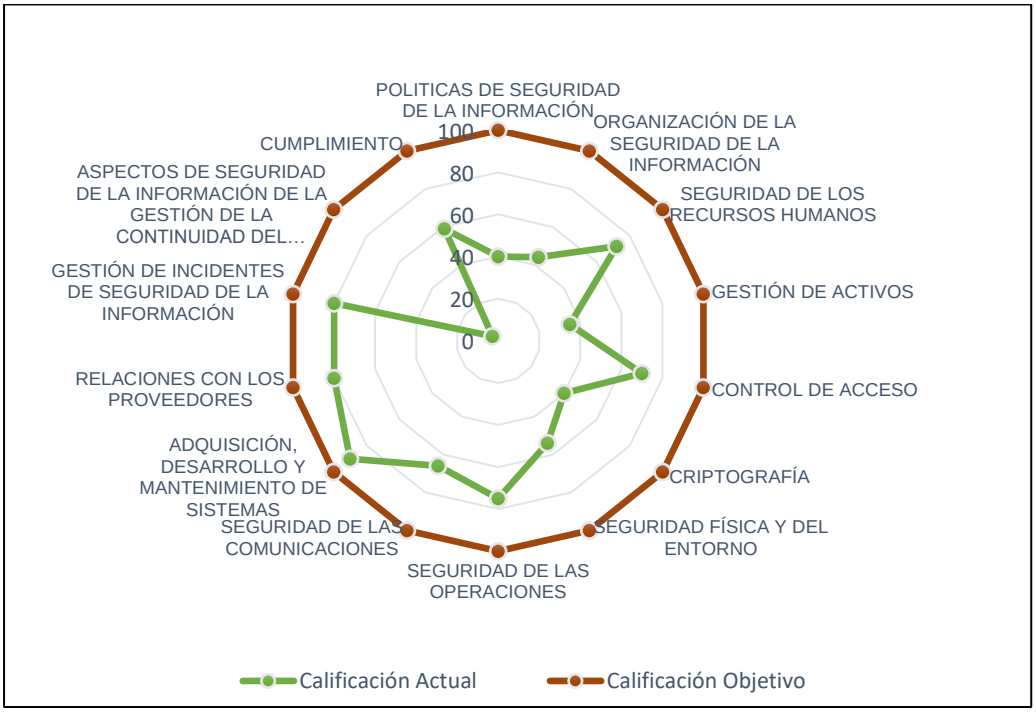


Tabla 32 Soporte de los Sistemas de Información

No.	Evaluación de Efectividad de controles			
	Dominio	Calificación Actual	Calificación Objetivo	Evaluación de Efectividad de Control
A.5	Políticas De Seguridad De La Información	40	100	**Repetible**
A.6	Organización De La Seguridad De La Información	44	100	**Efectivo**
A.7	Seguridad De Los Recursos Humanos	72	100	**Gestionado**
A.8	Gestión De Activos	35	100	**Repetible**
A.9	Control De Acceso	70	100	**Gestionado**
A.10	Criptografía	40	100	**Repetible**
A.11	Seguridad Física Y Del Entorno	54	100	**Efectivo**
A.12	Seguridad De Las Operaciones	75	100	**Gestionado**
A.13	Seguridad De Las Comunicaciones	66	100	**Gestionado**
A.14	Adquisición, Desarrollo Y Mantenimiento De Sistemas	90	100	**Optimizado**
A.15	Relaciones Con Los Proveedores	80	100	**Gestionado**
A.16	Gestión De Incidentes De Seguridad De La Información	80	100	**Gestionado**
A.17	Aspectos De Seguridad De La Información De La Gestión De La Continuidad Del Negocio	4	100	**Inicial**
A.18	Cumplimiento	59	100	**Efectivo**
PROMEDIO EVALUACIÓN DE CONTROLES		**58**	**100**	**EFECTIVO**

Fuente: Elaboración propia SISAM

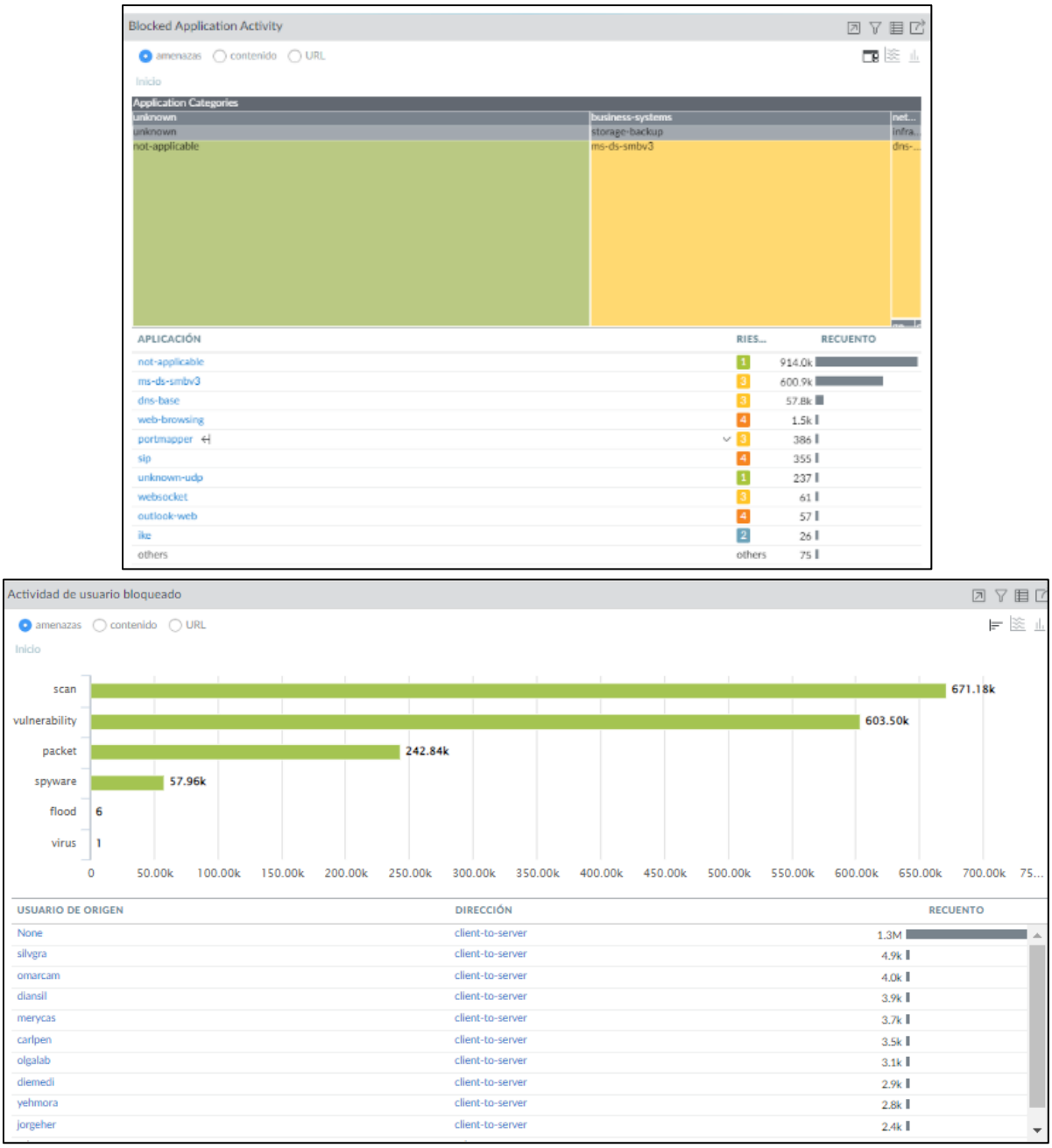
Con lo anterior se definen estrategias que permitan avanzar en la implementación de los diferentes dominios, para lo cual la Dirección General de Sanidad Militar definirá actividades que busquen fortalecer el Modelo de Seguridad y Privacidad de información, a continuación, se presentan las actividades formuladas durante la vigencia con el fin de fortalecer los dominios correspondientes Políticas de Seguridad de la Información, Organización de la Seguridad de la Información, Gestión de Activos, para lo cual el Área de Seguridad de Información realizara un autoevaluación en el último trimestre con el fin de revisar el avance en la implementación de las estratégicas y dominios priorizados.

Dentro de la vigencia el Grupo Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones – SISAM ha implementado herramientas y procedimientos que permiten la mitigación monitoreo y corrección a amenazas hacia la infraestructura de la red de la Dirección General, a continuación, se presenta algunas de las acciones realizadas del último trimestre 2024.

8.7.1. Acciones Correctivas Firewall

- Top 10 de las aplicaciones en las cuales se ha contabilizado las amenazas bloqueadas a través de la red de la DIGSA, discriminado por categoría de Riesgo, este monitoreo se ejecutó durante los últimos 90 días.

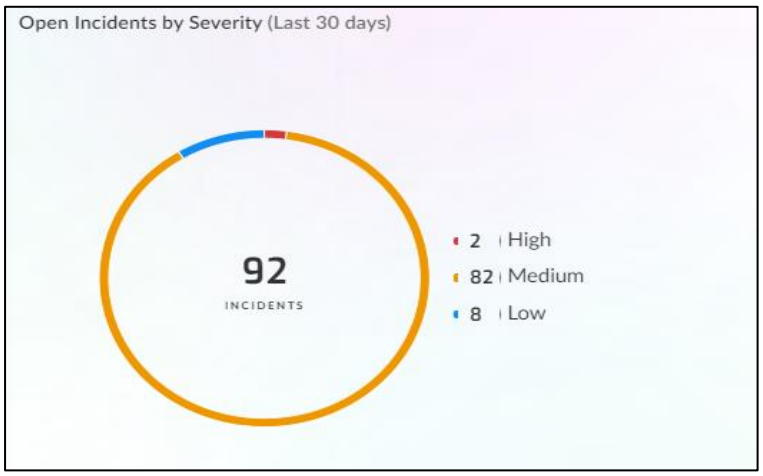
Ilustración 14. Acciones Correctivas Firewall



Fuente: Elaboración propia GRUGI

8.7.2. Monitoreo CORTEX XDR

Reporta la cantidad de las amenazas bloqueadas por la Solución de Seguridad CORTEX XDR instalada en los equipos de los funcionarios de la DIGSA, agrupadas por categoría Critica, Alta, Media y Baja, este monitoreo se ejecutó durante los últimos 90 días.



- Top 10 de los incidentes bloqueados por la Solución de Seguridad CORTEX XDR instalada en los equipos de los funcionarios de la DIGSA, discriminados por categoría y cantidad tales como: Critica, Alta, Media y Baja con su respectiva descripción de eventos como: Malware, Inyección, Script, PowerShell, DCSync y Digital Signer Restriction, este monitoreo se ejecutó durante los últimos 90 días.

Ilustración 15.Seguridad CORTEX XDR

Top Incidents (Top 10)

Score	Severity	Description	Alerts Breakdown	
80	M	'Digital Signer Restriction' along with 149 other alerts generated by XDR Agent detected on host digs...	150	[150]
80	M	111 'Digital Signer Restriction' alerts detected by XDR Agent on host digsagruga3102	111	[111]
80	M	99 'Digital Signer Restriction' alerts detected by XDR Agent on host digsaartsa2302	99	[99]
80	M	'Digital Signer Restriction' along with 86 other alerts generated by XDR Agent detected on host digsa...	87	[87]
80	M	'Digital Signer Restriction' along with 65 other alerts generated by XDR Agent detected on host digsa...	66	[66]
80	M	40 'Digital Signer Restriction' alerts detected by XDR Agent on host digsagruga3116	40	[40]
80	M	'Digital Signer Restriction' along with 31 other alerts generated by XDR Agent detected on host digsa...	32	[32]
80	M	24 'Digital Signer Restriction' alerts detected by XDR Agent on host dgsm-casiopera	24	[24]
80	M	'Digital Signer Restriction' along with 21 other alerts generated by XDR Agent detected on 2 hosts inv...	22	[22]
80	M	'Digital Signer Restriction' along with 15 other alerts generated by XDR Agent detected on host digsa...	16	[16]

Fuente: Elaboración propia GRUGI

9. Situación deseada u objetivo

9.1. Estrategia de TI

9.1.1. Misión Proyectados

Gestionar eficientemente lo servicios y recursos tecnológicos de la Dirección General de Sanidad Militar de Sanidad Militar, garantizando la oportunidad, disponibilidad, accesibilidad de los sistemas de información, soportado en una infraestructura tecnológica que permita la continuidad de sus servicios, garantizando cobertura, acceso a todos su usuarios, lo anterior en el marco de los habilitadores de arquitectura, seguridad y privacidad de la información, cultura y apropiación, Servicios de Ciudadanos Digitales de la política de

gobierno digital, igualmente desarrollar tecnologías emergentes, a través de la implementación de plan de transformación digital.

9.1.2. Visión Proyectados

El Subsistema de Salud de las Fuerzas Militares en el 2030, alcanzará una transformación significativa en sus procesos a partir de las capacidades digitales habilitadas para facilitar que sea una entidad que generará confianza a los usuarios en la prestación de los servicios integrales de salud y en el mantenimiento de la salud operacional, con eficiencia y calidad, con un equipo humano calificado y comprometido con el aseguramiento de su misionalidad.

9.1.3. Objetivo General Proyectados

Mejorar la prestación de los Servicios Tecnológicos a los grupos sociales de la Dirección General de Sanidad Militar – DIGSA.

9.1.3.1. Objetivos Específicos Proyectados

- Proveer un Sistema de Información Integrado, que permita la consolidación, análisis y gestión del flujo de información, para la toma de decisiones.
- Propender por la actualización de los servicios tecnológicos de la DIGSAS Invertir en tecnología de punta, como la integración de sistemas, la inteligencia artificial en el análisis de datos clínicos y telemedicina.
- Fortalecer el conocimiento tecnológico de los servidores públicos de DIGSA
- Mejorar la eficiencia operativa y aumentar la accesibilidad a los servicios de salud, especialmente en áreas remotas o de difícil acceso.

9.1.4. Capacidades de TI Proyectados

Categoría	Capacidad	Fortalecer o Desarrollar
Estrategia	Gestionar Arquitectura Empresarial	Desarrollar
	Gestionar Proyectos de TI	Fortalecer
	Definir Políticas de TI	Fortalecer
Gobierno	Gestionar Procesos de TI	Fortalecer
Sistemas de Información	Definir Arquitectura de Sistemas de Información	Fortalecer
	Administrar Sistemas de Información	Fortalecer
	Interoperar	Desarrollar
Infraestructura	Gestionar Disponibilidad	Fortalecer
	Realizara Soporte a Usuarios	Fortalecer
	Gestionar Cambios	Fortalecer
	Administrar Infraestructura Tecnológica	Fortalecer
Uso y Apropiación	Apropiar TI	Desarrollar
Seguridad de la Información	Diagnostico MSP	Desarrollar
	Definir Políticas SI	Desarrollar
	Gestión Riesgos SI	Fortalecer

Fuente: Elaboración propia SISAM

9.1.5. Servicios de TI Proyectados

Tabla 33 Soporte de los Sistemas de Información

ID	001	
Nombre	Acceso a la intranet	Acciones en el servicio de TI
Descripción	Suministra conectividad a la red global de datos a través de diferentes tecnologías y proveedores de servicio, permitiendo a los usuarios navegar, comunicarse y acceder a recursos en línea.	Configuración e Instalación AP Monitorear la estabilidad de la infraestructura.
Categoría	Conectividad	
Usuario objetivo	Funcionarios, contratistas de la Dirección General de Sanidad Militar y usuarios externos.	Configurar y definir políticas de seguridad.
Horario de prestación del servicio	24 horas, 7 días a la semana	
Canal de soporte	• Correo electrónico • Software de mesa de servicio	
Acuerdo de nivel de servicio	100% Proveedor	
Hallazgos u oportunidades de mejora	Mejorar la continuidad del Servicio Revisión Disponibilidad	

ID	002	
Nombre	Adquisición de licencias de software	Acciones en el servicio de TI
Descripción	Servicio de adquisición de licencias de software requeridas para usar en los diferentes procesos de la organización	Continuar con los Acuerdos Marco de Precio teniendo en cuenta el Tipo de Contratación, según lineamientos de Colombia Compra Eficiente.
Categoría	Gestión de recursos	
Usuario objetivo	Área de TI	
Horario de prestación del servicio	8 horas, 5 días a la semana	Actualizar inventario de licenciamiento de Software.
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Formulario en papel • Verbal	Revisión y actualización de aplicaciones.
Acuerdo de nivel de servicio	100% Proveedores	
Hallazgos u oportunidades de mejora	Revisión de criterios de Soporte por parte de Proveedores. Implementar Nivel Acuerdo de Servicios Interno	

ID	003	
Nombre	Correo electrónico junto con las herramientas colaborativas	Acciones en el servicio de TI Realizar Capacitación Monitorear Plataforma. Actualizar y Configurar
Descripción	Permite a los usuarios enviar, recibir y gestionar mensajes electrónicos de manera eficiente y segura, facilitando la comunicación interna y externa dentro de la entidad	
Categoría	Comunicación	
Usuario objetivo	Funcionarios y contratistas de la entidad	
Horario de prestación del servicio	24 horas, 7 días a la semana	
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Formulario en papel • Verbal	
Acuerdo de nivel de servicio	100% Proveedores	
Hallazgos u oportunidades de mejora	Implementar Nivel Acuerdo de Servicios Interno	

ID	004	
Nombre	Gestión de red de infraestructura tecnológica	Acciones en el servicio de TI Monitorear estabilidad de la infraestructura tecnológica. Actualización Roles Configuración y Actualización. Realizar actualizaciones o modernización de infraestructura.
Descripción	Gestión de la administración y configuración centralizada de la seguridad de la red que usan los Sistemas de información	
Categoría	Gestión de recursos	
Usuario objetivo	Entidad	
Horario de prestación del servicio	24 horas, 7 días a la semana	
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Formulario en papel • Verbal	
Acuerdo de nivel de servicio	100% Proveedores	
Hallazgos u oportunidades de mejora	Implementar Nivel Acuerdo de Servicios Interno	

ID	005	
Nombre	Telefonía IP	Acciones en el servicio de TI Monitorear estabilidad de la infraestructura tecnológica.
Descripción	Servicio de comunicaciones telefónicas entre usuarios internos y externos de la institución.	
Categoría	Comunicación	
Usuario objetivo	Funcionarios y contratistas de la entidad	

ID	005	
Horario de prestación del servicio	24 horas, 7 días a la semana	Configuración y Actualización.
Canal de soporte	• Correo electrónico • Software de mesa de servicio • IVR • Formulario en papel • Verbal	
Acuerdo de nivel de servicio	100% Proveedores	
Hallazgos u oportunidades de mejora	Implementar Nivel Acuerdo de Servicios Interno	

ID	006	
Nombre	Servicio de antivirus	Acciones en el servicio de TI Actualizar directivas, roles, políticas. Monitorear Plataforma y Gestión de Incidencias. Verificar en los clientes la actualización.
Descripción	Software que detecta y elimina virus y otras amenazas informáticas en la red, sistemas de información, PC, dispositivos móviles y demás.	
Categoría	Seguridad	
Usuario objetivo	Entidad	
Horario de prestación del servicio	24 horas, 7 días a la semana	
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Formulario en papel • Verbal	
Acuerdo de nivel de servicio	100%	
Hallazgos u oportunidades de mejora	Implementar Nivel Acuerdo de Servicios Interno	

ID	007	
Nombre	Servicio de entrenamiento y capacitación uso de las soluciones de TI	Acciones en el servicio de TI Identificar las necesidades de capacitación en los grupos interno de trabajo DIGSA. Ejecutar capacitación plan de capacitación.
Descripción	Servicio que suministra capacitación y entrenamiento sobre las funciones de los sistemas de información que maneja la entidad.	
Categoría	Gestión recursos	
Usuario objetivo	Área de TI	
Horario de prestación del servicio	8 horas, 5 días a la semana	
Canal de soporte	• Correo electrónico • Software de mesa de servicio	

ID	007	
	• Formulario en papel • Verbal	
Acuerdo de nivel de servicio	De acuerdo con estimación	
Hallazgos u oportunidades de mejora	Implementar Nivel Acuerdo de Servicios Interno	

ID	008	
Nombre	Plataforma de Mesa de servicio	Acciones en el servicio de TI Implementar Nivel Acuerdo de Servicios para requerimiento de soporte técnico e integral en sitio. Implementar Nivel Acuerdo de Servicios funcional Sistemas de Información.
Descripción	Plataforma para registro, consulta y respuesta de peticiones, quejas, reclamos, sugerencias y denuncias.	
Categoría	Aplicación	
Usuario objetivo	• Funcionarios y contratistas de soporte, • Funcionarios y contratistas que generan PQR	
Horario de prestación del servicio	24 horas, 7 días a la semana	
Canal de soporte	• Correo electrónico • Software de mesa de servicio • IVR • Formulario en papel • Verbal	
Acuerdo de nivel de servicio	100% Proveedores	
Hallazgos u oportunidades de mejora	Implementar Nivel Acuerdo de Servicios Interno	

ID	009	
Nombre	Gestión de equipos de cómputo	Acciones en el servicio de TI Diagnosticar la falla presentada (incidencia o falla definitiva). · Informar al supervisor del contrato. Determinar si se requiere el remplazo de la parte o su reparación. Cambiar la parte por una nueva (suministrada por DIGSA) o repararla e instalarla nuevamente si es el caso. Determinar tiempo de instalación y funcionamiento. · Realizar el reporte técnico, detallando si se requiere un
Descripción	Adquisición, instalación, configuración y mantenimientos preventivos y correctivos de hardware y software de los equipos asignados a los funcionarios y contratistas de la Entidad	
Categoría	Gestión de recursos	
Usuario objetivo	Funcionarios y contratistas de la entidad	
Horario de prestación del servicio	8 horas, 5 días a la semana	
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Formulario en papel • Verbal	
Acuerdo de nivel de servicio	100% Proveedores	

ID	009	
Hallazgos u oportunidades de mejora	Implementar Nivel Acuerdo de Servicios Interno	cambio de repuesto (suministro a cargo de DIGSA) y su estado.

ID	010	
Nombre	Servicios de Instalación de software en Equipos de computo	**Acciones en el servicio de TI**
Descripción	Instalación de software por demanda en los equipos de cómputo de los funcionarios o contratistas	Recibir las solicitudes para soporte técnico por los grupos internos de trabajo para la instalación de Equipos de cómputo y/o Software. Validar licenciamiento Software y disponibilidad de Equipos. Realizar las instalaciones de acuerdo a la disponibilidad.
Categoría	Gestión de recursos	
Usuario objetivo	Funcionarios y contratistas de la entidad	
Horario de prestación del servicio	8 horas, 5 días a la semana	
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Formulario en papel • Verbal	
Acuerdo de nivel de servicio	8 horas diarias hábiles	
Hallazgos u oportunidades de mejora	Implementar Nivel Acuerdo de Servicios Interno	

Fuente: Elaboración propia SISAM

9.1.6. Otros Servicios de TI Proyectados

Como parte de la estrategia del Plan Estratégico Institucional PEI 2023 - 2026 el cual proyecta "Adoptar la transformación digital en cumplimiento a la política de gobierno digital". Para alcanzar la transformación digital, inicialmente se ha concentrado esfuerzos en inversión de Ciberseguridad, Uso de nube- Software como servicio - Microsoft 365, Máquinas virtuales (Virtualización de hardware), entre otras.

La inversión en estas tecnologías emergentes brindan herramientas que coadyuven en el cumplimiento de la misión y las políticas institucionales dentro de un entorno digital; la tabla a continuación *"*Tecnologías 4R tendencias 2026*"* muestra como los procesos del DIGSA proyectan la necesidad de uso y apropiación a futuro de estas tecnologías, abordando la primera fase que se pretende implementar por medio de herramientas de nube, sin embargo se requiere establecer un presupuesto importante para elaborar una hoja de ruta que proyecte el uso de tecnologías de la cuarta revolución industrial como lo son:

1. Análisis masivo de datos (Big data),
2. Inteligencia Artificial (AI),
3. Internet de las Cosas (IoT),
4. Robótica y similares,
6. Automatización robótica de procesos
7. Cartografía- georreferenciación -visores
8. Ciberseguridad
9. Otras tecnologías 4RI

Todas estas tecnologías mencionadas anteriormente para TD, procesos realizo un proceso de investigación muy completo (ver anexo 1) adjunto resumen por necesidad por proceso:

Tabla 34 Tecnologías 4R tendencias 2026

TECNOLOGIAS 4RI TENDENCIA										
AREAS DIGSA	Herramientas BI	Bases de datos	Power BI	Mapinfo-google-arcgis	Power Automate	Firma digital	Tableau	Office azure	Plataf. Colaborativa	Block Chain
ARCOM	1									
GRAPS	1				1					
GRERI	1	1	1	1	1					
GROSD	1	1	1	1						
GRSYE										
GRUAA						1				
GRUAS		1		1		1	1	1		
GRUCO						1			1	1
GRUFI									1	
GRUGA	1	1	1	1						
GRUGI	1	1								
GRULE										1
GRUPL	1		1							
GRUSO	1	1	1	1			1	1		
GRUTH	1			1						
SISAM			1		1					
TOTAL	9	6	6	6	3	3	2	2	2	2
% uso y apropiación	56	38	38	38	19	19	13	13	13	13

Fuente: GRUGI Capacitación 2024

9.2. Tablero de control de TI Proyectado

Dentro de la situación deseada se proyecta la implementación de otros indicadores que permita el monitorear la gestión TI, a continuación, se presentan el consolidado de indicadores proyectados a implementar:

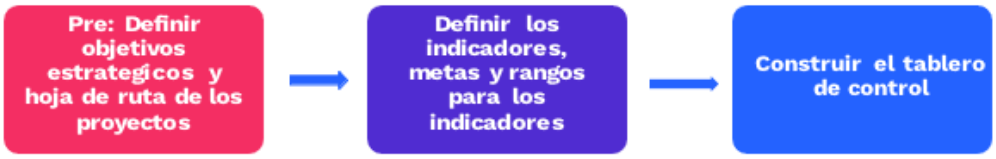
Tabla 35 Tablero de control de TI Proyectado 2026

ID	TIPO	INDICADOR	%	FORMULA	VARIABLES	FRECUENCIA
1	Operación	Índice de disponibilidad de aplicativo WEB	**ID**	ID= (TSA-TB) /TSA*100)	**TSA**=Tiempo de servicio acordado **TB**= sumatorio de los tiempos sin servicio	Trimestral
2	Operación	Índice 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
3	Operación	Cumplimiento de los ANS de proveedores	**IC**	IC= (SE / SP) *100)	**SE**= # de servicios planeados en periodo analizado S**E**= # de servicios ejecutados en periodo analizado	Semestral
4	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	Semestral
6	Estratégicos	Variación en trámites atendidos	**PAT**	AT = (TA / NT) *100	**NT**: Total de trámites que tiene la entidad **TA**: Trámites Autorizados en la entidad.	Trimestral

ID	TIPO	INDICADOR	%	FORMULA	VARIABLES	FRECUENCIA
7	Estratégicos	Cumplimiento presupuestal funcionamiento de TI	**VTA**	VTA = ((TT - TA) / TA) *100	**TT**: No. total de trámites atendidos en el actual período. **TA:** No. total de trámites atendidos en el anterior período.	Trimestral
8	Resultado	Disponibilidad de Sistemas de Información	**DSI**	DSI = ((TSA – TB) / TSA) *100	D = Porcentaje de disponibilidad de los sistemas de información en operación durante el intervalo de tiempo analizado. TSA: Tiempo de servicio acordado. TB: Sumatoria de los tiempos sin servicio.	Mensual
9	Resultado	Porcentaje de procesos críticos de TI monitoreados	**PPCM**	PPCM = (PCM / PC) * 100	PPCM: Porcentaje de procesos críticos de TI monitoreados PCM: Número de procesos críticos de TI monitoreados PC: Total procesos críticos de TI	Semestral
10	Resultado	Porcentaje de implementación de requerimientos de los sistemas de información	**PRSI**	PRSI = (RI/RE) *100	PRSI = Porcentaje cumplimiento requerimientos de sistemas de información. RI: Número de requerimientos sobre sistemas de información implementados, durante el período de tiempo analizado. RE: Número de solicitudes de implementación de requerimientos planeadas para ser implementadas, durante el período de tiempo analizado.	Mensual

Fuente: Elaboración propia SISAM

Igualmente, como fortalecimiento a los procesos misionales, estratégico y de apoyo se proyecta tableros de control con el fin de fortalecer sus procedimientos y la gestión en cumplimiento de sus objetivos y alcance, el proceso para el levantamiento y diseño se realizar en mesas de trabajo con los grupos internos de trabajo, y se tendrá la siguiente secuencia para su construcción.



9.3. Modelo de Gestión y Gobierno de TI Proyectado

Con el fin de avanzar en el Marco de Arquitectura Empresarial se plantea iniciar con la implementación del Modelo de Gestión y Gobierno de TI, continuación se presentan las actividades priorizadas en cada uno de los siete dominios que conforman el modelo.

Ilustración 16. Modelo de Gestión y Gobierno de TI - MGGTI

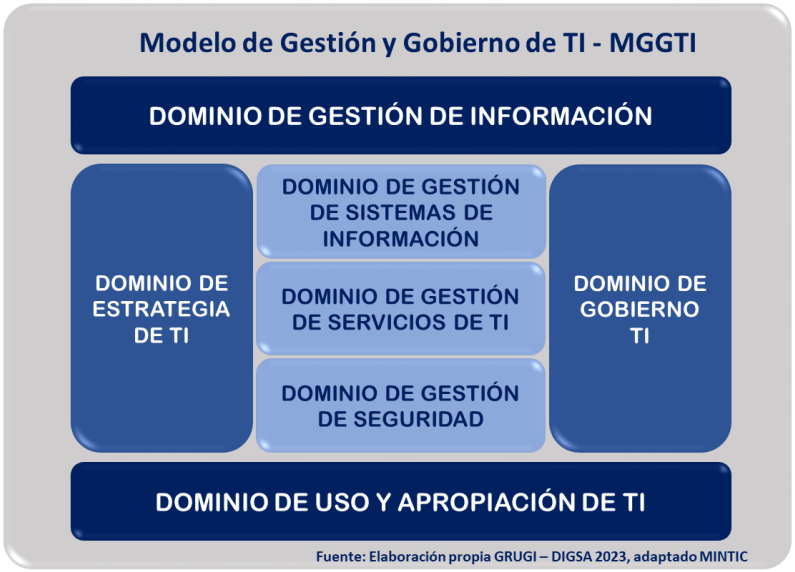


Tabla 36 . Modelo de Gestión y Gobierno de TI Proyectado

Dominio / Proceso	Lineamiento	Descripción de la Actividad
Dominio de Estrategia de TI	MGGTI.LI.ES.01 Entendimiento Estratégico de TI	Documento de alineación de la estrategia de la DIGSA con la estrategia de TI (Documento de Entendimiento estratégico y Oportunidades y Necesidades de TI)
	MGGTI.LI.ES.02 Documentación de la Estrategia de TI	Plan Estratégico de las Tecnologías de la Información PETI, el cual debe contener la proyección de la estrategia para 2 años
	MGGTI.LI.ES.04 Gestión del presupuesto de TI	Matriz o tablero de control de planeación de recursos financieros, con su apropiación, compromiso, pago y saldos. Atado al Plan Anual de Adquisiciones y la disposición de vigencias futuras.
	MGGTI.LI.ES.05 Catálogo de servicios de TI	Catálogo de servicios de TI actualizado, con los Acuerdos de Nivel de Servicio (ANS) asociados
Dominio de Gobierno de TI	MGGTI.LI.GO.01 Esquema de gobierno de TI	Documento que recoge la estrategia de gobierno y gestión de TI, la cual incluye el detalle de políticas, estructura organizacional, definiciones de diseño de la estructura, grupos e instancias de coordinación
	MGGTI.LI.GO.04 Gestión de cambios	Proceso de Gestión de Cambios documentado y formalizado en el Sistema de Gestión de Calidad de la Entidad
	MGGTI.LI.GO.08 Mejoramiento de los procesos	Documentos actualizados del proceso de gestión de TI subprocesos, procedimientos, guías y documentación de TI.
	MGGTI.LI.GO.09 Gestión de Proveedores de TI	Evidencias de las acciones de los supervisores en la gestión de los procesos contractuales en el que se evidencie la gestión y seguimiento tendiente a dar cumplimiento a la calidad y cantidad de los bienes y servicios contratados

Dominio / Proceso	Lineamiento	Descripción de la Actividad
Dominio de Gestión de Información	MGGTI.LI.GI.01 Gobierno de datos	Esquema de gobierno de datos con: Políticas y principios; Roles y responsabilidades; instancias de toma de decisiones, estándares a aplicar, indicadores, modelo de gestión de datos actualizado.
	MGGTI.LI.GI.07 Uso del código postal colombiano	Sistemas de información y formatos que incorporan campos para registro del código postal de la República de Colombia.
	MGGTI.LI.GI.08 Explotación de datos	Ejercicios de analítica descriptiva, predictiva, o prospectiva, y tableros de control con información que soporte la toma de decisiones de la Entidad.
Dominio de Gestión de Sistemas de Información	MGGTI.LI.SI.01 Metodología para el desarrollo de sistemas de información	Documento, manual o procedimiento que defina la metodología para el desarrollo y mantenimiento de software alineada a las mejores prácticas. Evidencia de aplicación de metodología de desarrollo de software en caso de desarrollo por parte de un tercero.
	MGGTI.LI.SI.02 Catálogo de Sistemas de Información	Catálogo de Sistemas de Información actualizado, (producto tipo disponible en micrositio de arquitectura de MinTIC).
	MGGTI.LI.SI.04 Ambientes independientes en el ciclo de vida de los sistemas de información	Vista de separación de ambientes. Esquema de operación y control cambios donde se especifique un protocolo de paso de versiones entre ambiente.
	MGGTI.LI.SI.05 Análisis de requerimientos de los sistemas de información	Guía o procedimiento donde se definan actividades para la identificación, levantamiento, análisis, validación y trazabilidad de los requerimientos, de acuerdo con la metodología adoptada por la Entidad. Formatos, artefactos y/o herramientas donde se lleve el ciclo de vida de los requerimientos, contemplando las siguientes etapas: Identificación, Especificación, Calidad, Análisis, Validación, Trazabilidad.
	MGGTI.LI.SI.07 Plan de pruebas durante el ciclo de vida de los sistemas de información	Plan de pruebas de nuevos desarrollos o mantenimientos evolutivos debe contar con planes de pruebas funcionales y no funcionales. Documentos, artefactos, informes o actas que evidencien la aprobación de las pruebas por las partes involucradas.

Dominio / Proceso	Lineamiento	Descripción de la Actividad
	MGGTI.LI.SI.08 Manual del usuario, técnico y de operación de los sistemas de información	Manual de usuario, se recomienda incluir en la Documentación/artefactos para usuarios debe contener y/o hacer referencia: • La descripción del sistema de información. • El objetivo del sistema de información. • Los procesos de negocio y las áreas que soporta. • La descripción de los módulos y funcionalidades que lo componen. • El uso de las funcionalidades del sistema de información. • Errores funcionales más comunes y su solución. Manual técnico y de operación: debe contener y/o hacer referencia: • Errores técnicos más comunes y su solución. • Descripción de despliegue y configuración de los componentes que conforman el sistema de información.
	MGGTI.LI.SI.12 Requerimientos no funcionales o atributos calidad de los sistemas de Información	Documento de especificación de requerimientos no funcionales (atributos de calidad).
	MGGTI.LI.SI.13 Accesibilidad	Trámites, servicios, sistemas de información que incorporen las buenas prácticas relacionadas con la accesibilidad web.
	MGGTI.LI.SI.14 Arquitectura de Software	Documentación de la Arquitectura de Software de cada uno de los sistemas de información, que al menos incluya: • Vista conceptual que describe el sistema en términos de sus principales elementos de diseño y las relaciones entre ellos. • Vistas integración e interoperabilidad. • Vista de operación que describa la estructura dinámica de un sistema. • La estructura del código describe cómo se organizan el código fuente, los binarios y las bibliotecas en el entorno de desarrollo.
Dominio de Gestión de Servicios de TI	MGGTI.LI.ST.01 Catálogo de servicios de Tecnología	Catálogo de servicios de Tecnología
	MGGTI.LI.ST.05 Alta disponibilidad de los Servicios de TI	Infraestructuras y servicios de alta disponibilidad implementadas para garantizar la continuidad del servicio.
	MGGTI.LI.ST.07 Acuerdos de Nivel de Servicios	Contratos de servicios con ANS incluidos. Informe o indicadores de cumplimiento de ANS.

Dominio / Proceso	Lineamiento	Descripción de la Actividad
	MGGTI.LI.ST.08 Soporte a los servicios de TI	Mesa de servicio implementada. Procedimiento de gestión de requerimientos e incidentes definido e implementado.
	MGGTI.LI.ST.10 Monitoreo de la infraestructura de TI	Procedimientos y mecanismos de monitoreo de los recursos de la infraestructura de TI.
	MGGTI.LI.ST.11 Respaldo y recuperación de los Servicios tecnológicos	Plan de respaldo y recuperación ante desastres. Evidencias de prueba de consistencia de las copias de respaldos.
Dominio de Gestión de Seguridad	MGGTI.LI.GS.01 Modelo de Seguridad y Privacidad de la Información	Evidencias de la gestión e implementación del modelo de seguridad de la información conforme a las salidas y evidencias que definió el Modelo MSPI de MinTIC.
	MGGTI.LI.GS.02 Gestión de riesgos de seguridad	Matriz de riesgos de seguridad para los activos de información de la entidad (sistemas de información, infraestructura de TI, datos e información, procesos, personas, entre otros). Plan de tratamientos de riesgos de seguridad de la información. Evidencias de manejo y gestión de riesgos cuando se materializan.
	MGGTI.LI.GS.03 Gestión de controles de seguridad	Matriz de controles de seguridad definidos para los activos de información. Evidencias de la implementación de los controles definidos.
	MGGTI.LI.GS.04 Monitoreo de seguridad	Herramientas de monitoreo de seguridad implementadas y configuradas. Indicadores de seguridad digital identificados y gestionados a través de tableros de control.
Dominio de Uso y Apropiación de TI	MGGTI.LI.UA.01 Estrategia de Uso y Apropiación de TI	Estrategia de uso y apropiación de TI definida y evidencias de su implementación.

Fuente: Elaboración propia SISAM

9.3.1. Gestión de Servicios de TI Proyectado

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.

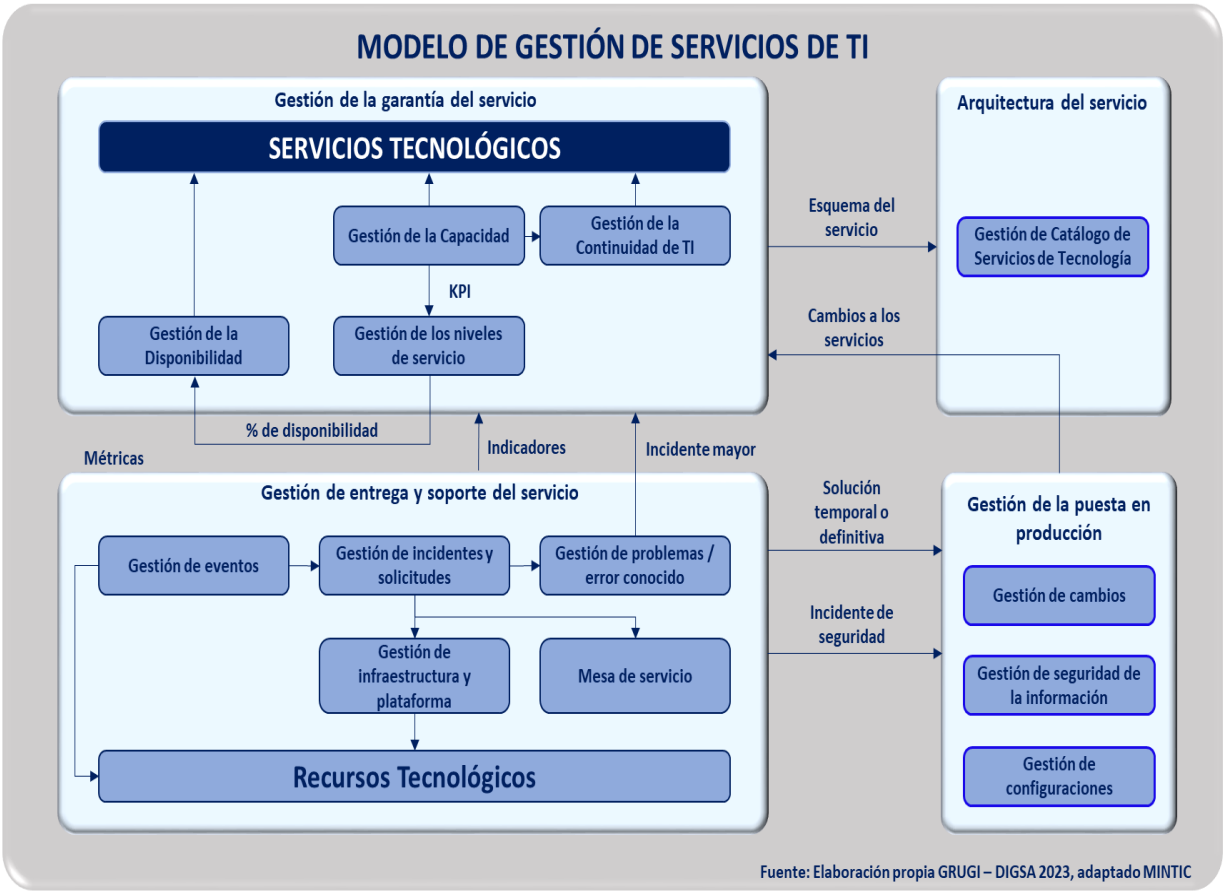
- Debe garantizar la continuidad y disponibilidad de los servicios de TI, así como la capacidad de atención y resolución de incidentes para ofrecer continuidad de la operación y la prestación de todos los servicios de la entidad y de TI.

- 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 17. Modelo Gestión de servicios TI



9.3.2. Gestión y Supervisión del Presupuesto Inversión objetivo

Tabla 37. Iniciativas y Proyectos objetivo

CATEGORIA	PRODUCTO	ACTIVIDADES DEL PROYECTO (FICHA EBI)	PRESUPUESTO 2025
SOFTWARE	SERVICIOS DE INFORMACIÓN ACTUALIZADOS	DESARROLLAR MÓDULO DE VERTICAL DE SALUD	$ 1.316.507.273,13
		Servicio de fábrica de software, encaminado a efectuar desarrollar ajustes a cambios normativos y módulos de cirugía, hospitalización, enfermería y urgencias.	$ 316.507.273,13
		Actualización capa de aplicación y arquitectura de datos	$ 500.000.000,00
		Continuación desarrollo e implementación ecosistema de interoperabilidad con red prestadora de servicios de salud	$ 500.000.000,00
SERVICIOS	SERVICIOS TECNOLÓGICOS	GESTIONAR LA ADQUISICIÓN DEL SERVICIO DE DATACENTER PARA EL DESARROLLO E IMPLEMENTACIÓN DEL SISTEMA DE INFORMACIÓN A NIVEL NACIONAL	$ 1.302.545.085,88
		Servicio de DATACENTER MDN (Productivo y continuidad de negocio)	$ 1.302.545.085,88
		REALIZAR SOPORTE TÉCNICO (MANTENIMIENTO SOFTWARE, MESA DE SERVICIO)	$ 1.700.000.000,00
		Contratación servicio de soporte y mantenimiento de software	$ 1.300.000.000,00
		Contratación servicio de mesa de ayuda	$ -
SERVICIOS		Contratación soporte y mantenimiento plataforma PACS integrada (DIGSA - FAC)	$ 400.000.000,00
TOTALES			$ 4.319.052.359,00

Fuente: Presupuesto SISAM 2024

Ilustración 18.Plan de inversión SALUD: SIS 2025

ACTIVIDAD	PRESUPUESTO 2025
DESARROLLAR MODULO DE VERTICAL DE SALUD	$ 1.316.507.273,13
SERVICIO DE DATACENTER MDN	$ 1.302.545.085,88
SOPORTE TÉCNICO EVOLUTIVO	$ 1.700.000.000,00
TOTAL	$ 4.319.052.359,00

Fuente: Elaboración propia SISAM

9.3.3. Gestión y Supervisión del Presupuesto funcionamiento objetivo

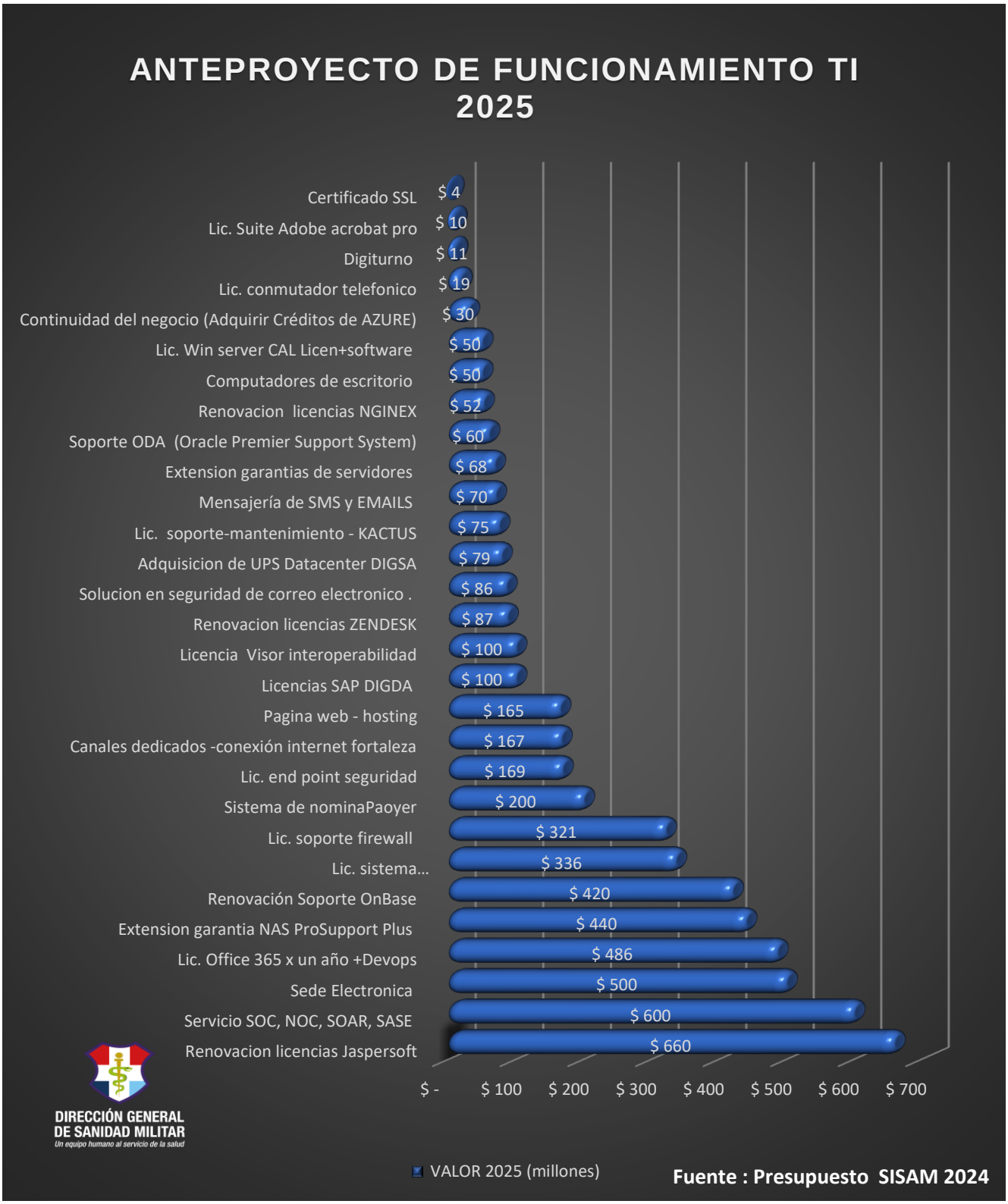
Tabla 38 Presupuesto funcionamiento objetivo

TEM	NECESIDAD	VALOR 2025
1	Computadores de escritorio	$ 50.000.000
2	Licenciamiento conmutador telefónico	$ 18.500.000
3	Licenciamiento soporte firewall	$ 321.000.000
4	Licenciamiento end point seguridad	$ 168.525.000
5	Solución en seguridad de correo electrónico.	$ 85.600.000
6	Servicio SOC, NOC, SOAR, SASE	$ 600.000.000
7	(Certificado SSL) 81112103	$ 3.500.000
8	Canales dedicados y conexión a internet fortaleza	$ 166.920.000
9	Continuidad del negocio - servicio en la nube (Adquirir Créditos de AZURE)	$ 30.000.000
10	Licenciamiento soporte y mantenimiento - KACTUS	$ 75.000.000
11	Licenciamiento de suite adobe Acrobat pro - licencia adobe stock	$ 9.630.000
12	Sistema de nómina Paoyer	$ 200.000.000
13	Licencias SAP DIGDA	$ 100.000.000
14	Licenciamiento Office 365 para servicios en la nube por un año + Devops	$ 486.400.000
15	Licenciamiento sistema operativo Datacenter	$ 336.000.000
16	Licenciamiento Winserver CAL License& software Assurance Open	$ 50.000.000

17	Extensión garantías de servidores	$	68.480.000
18	Página web - hosting	$	165.000.000
19	Extensión de garantía NAS Pro Support Plus	$	440.000.000
20	Soporte ODA (Oracle Premier Support for System) – Debe Incluir Cambio de Partes en Sitio	$	60.000.000
21	Renovación Soporte OnBase	$	420.000.000
22	Renovación licencias Jaspersoft	$	659.600.000
23	Renovación licencias NGINEX	$	52.000.000
24	Renovación licencias ZENDESK	$	87.200.000
25	Mensajería de SMS y EMAILS	$	70.000.000
26	Licencia Visor interoperabilidad	$	100.000.000
27	Digiturno	$	11.000.000
28	Adquisición de UPS Datacenter DIGSA	$	78.500.000
29	Sede Electrónica	$	500.000.000
	TOTAL	**$**	**5.412.855.000**

Fuente: Elaboración propia SISAM

Ilustración 19. Anteproyecto de presupuesto SISAM 2024



9.3.4. Gestión de Información Proyectado

Con el objetivo de Mejorar la Calidad de la Información y elevar los estándares de precisión, relevancia y confiabilidad de la información proporcionada a todos grupos interno de trabajo de la Dirección General de Sanidad Militar y que permita ser una base sólida para la toma de decisiones informadas y efectivas, se proponen llevarán a cabo las siguientes acciones clave:

- Estandarización de Datos: Establecer criterios y formatos estandarizados para la captura, almacenamiento y presentación de datos en el sistema de información integrado de la DIGSA, asegurando la coherencia y consistencia de la información en todos los niveles.

- Validación y Verificación de Datos: Implementar procesos y herramientas de validación y verificación de datos para garantizar su exactitud y fiabilidad, identificando y corrigiendo errores o inconsistencias de manera proactiva.

- Mejora de Procesos de Captura de Datos: Optimizar los procesos y herramientas de captura de datos en todas las áreas de la Entidad, mediante la automatización de tareas repetitivas, la eliminación de duplicidades y la simplificación de formularios y procedimientos.

- Garantía de Calidad de Datos: Establecer controles de calidad de datos para monitorear y mantener la integridad de la información a lo largo del tiempo, identificando y corrigiendo desviaciones o anomalías en los datos recolectados.

- Capacitación del Personal: Capacitar al personal de la DIGSA en la importancia de la calidad de la información y en las mejores prácticas para su recolección, almacenamiento y uso adecuado, promoviendo una cultura organizacional orientada a la excelencia en la gestión de datos.

Al mejorar la calidad de la información, la DIGSA podrá contar con herramientas de software y una base de datos confiable y precisa que respalde la toma de decisiones en todos los niveles de la institución. Esto permitirá una gestión más eficiente y efectiva de los recursos, una mayor capacidad de respuesta ante situaciones críticas y una mejora continua en la calidad de la atención médica proporcionada a las Fuerzas Militares y sus familias.

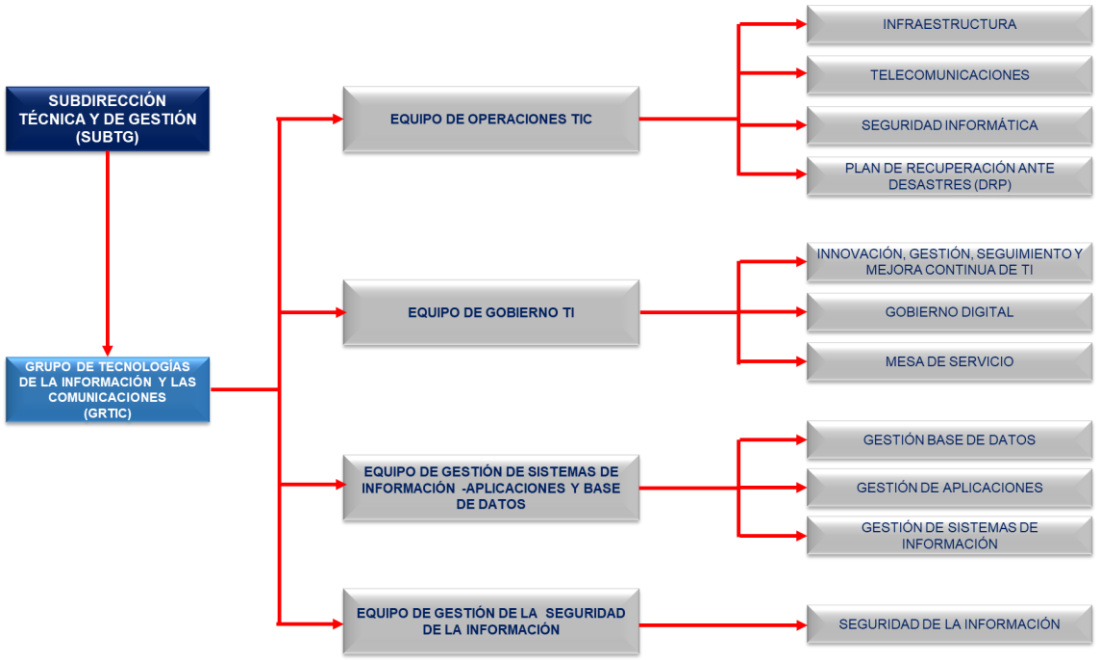
9.3.5. Estructura y Organización Humana de TI Proyectado

El objetivo es Liderar los aspectos relacionados con tecnologías de la información y las telecomunicaciones en la Entidad, convirtiéndonos en un habilitador para el cumplimiento de la misión y objetivos de esta, alineando la tecnología con los procesos de la organización.

Misión GRTIC: Apoyar la adopción y la implementación de las políticas del gobierno nacional en lo concerniente a las Tecnologías de Información y Comunicaciones TIC y asesorar a la Dirección de Sanidad de las Fuerzas Militares en su modernización y evolución tecnológica, brindando soluciones integrales en tecnologías de la información y comunicaciones que contribuyan al cumplimiento de la misión institucional.

Visión GRTIC: Al 2026 ser el área de la Dirección de Sanidad de las Fuerzas Militares con mayor promoción de la innovación tecnológica y el cambio institucional con la toma de decisiones basados en información, generando valor a la Dirección de Sanidad de las Fuerzas Militares a través del mejoramiento continuo.

Ilustración 20. Estructura y Organización Humana de TI Proyectado



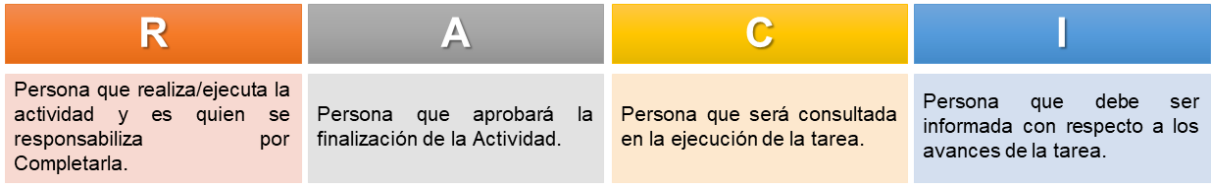
Fuente: Elaboración propia SISAM

9.3.6. Definición de Roles y Funciones del Grupo de Tecnologías de la Información y las Comunicaciones (GRTIC)

Para el cumplimiento de su misión el GRUPO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (GRTIC) contara con los siguientes roles y funciones:

1. Coordinador Grupo de Tecnologías De La Información Y Las Comunicaciones (GRTIC)
2. Apoyo Administrativo
3. Equipo De Operaciones TIC
   - Infraestructura
   - Telecomunicaciones
   - Seguridad informática
   - Plan de Recuperación Ante Desastres (DRP)
4. Equipo de Gobierno TI
   - Innovación, Gestión, Seguimiento Y Mejora Continua De TI
   - Gobierno Digital
   - Mesa de Servicio
5. Equipo De Gestión De Sistemas De Información Aplicaciones Y Base De Datos
   - Gestión Base De Datos
   - Gestión De Aplicaciones
   - Gestión De Sistemas De Información
6. Equipo de Gestión de la Seguridad de la Información
   - Seguridad De La Información

Ilustración 21. Modelo RACI



Fuente: Elaboración propia SISAM

Tabla 39. Matriz RACI SISAM

Funciones/Dependencias	Comité de Gestión y Desempeño	Coordinador SISAM	Equipo De Operaciones TIC	Equipo de Gobierno TI	Equipo De Gestión De Sistemas De Información Aplicaciones Y	Equipo de Gestión de la Seguridad de la Información
Operaciones TIC						
Asesorar a la Dirección General de Sanidad Militar en la planeación, diseño, implementación, promoción y administración de telecomunicaciones e informática para el mejoramiento continuo del servicio de sus afiliados.	I	R	C	C	C	C
Orientar y liderar de manera concertada el Plan Estratégico en informática respondiendo a las necesidades a la Dirección General de Sanidad Militar y alineando el modelo estratégico de la entidad con la tecnología	I	R	C	C	C	C
Gerenciar la implementación de los diversos proyectos de tecnología en telecomunicaciones e informática de la Dirección General de Sanidad Militar.	I/A	R	C	C	C	C
Desarrollar y poner en marcha los proyectos que respondan a las estrategias definidas en el Plan estratégico en Telecomunicaciones e informática, promoviendo el avance tecnológico en todos los niveles de la entidad	I/A	R	C	C	C	C
Asesorar y promover la contratación de Tecnología en telecomunicaciones e informática, así como, investigar y analizar tecnología de punta para satisfacer las necesidades de las diferentes oficinas y/o grupos, y poder definir racionalmente la inversión institucional	I	R	C	C	C	C

Funciones/Dependencias	Comité de Gestión y Desempeño	Coordinador SISAM	Equipo De Operaciones TIC	Equipo de Gobierno TI	Equipo De Gestión De Sistemas De Información Aplicaciones Y	Equipo de Gestión de la Seguridad de la Información
Promover y proponer mecanismos para el uso de la tecnología instalada de telecomunicaciones e informática que permita incrementar la efectividad y productividad de la Dirección General de Sanidad Militar	I/A	R	C	C	C	C
Administrar y supervisar el funcionamiento de Telecomunicaciones e informática de la Dirección General de Sanidad Militar de acuerdo con los nivele de servicio requeridos por la institución	I	R	C	C	C	C
Operaciones TIC						
Infraestructura: Encargado de la adquisición, instalación, soporte y mantenimiento de un sistema o servidor informático de cualquier tipo que utilice capacidad de procesamiento, almacenamiento o gestión de información. Evitar el tiempo de inactividad de los servidores antes mencionados o categorizados a través de un mantenimiento preventivo, correctivo o adaptativo programado, garantizando la seguridad de los servidores y la mayor disponibilidad posible.	I	C/A/R	R	C	C	C/A
Telecomunicaciones: Encargado de implementar y administrar la infraestructura de la red de voz, datos y eléctrica de la Dirección General de Sanidad Militar y que se encuentran bajo el gobierno del Grupo de Tecnologías De La Información Y Las Comunicaciones (GRTIC), con el fin de garantizar la conectividad y el servicio eléctrico	I	C/A/R	R	C	C	C/A
Seguridad informática: Encargado de proteger la disponibilidad, confidencialidad e integridad de las tecnologías de la información	I	C/A/R	R	C	C	A/C

Funciones/Dependencias	Comité de Gestión y Desempeño	Coordinador SISAM	Equipo De Operaciones TIC	Equipo de Gobierno TI	Equipo De Gestión De Sistemas De Información Aplicaciones Y	Equipo de Gestión de la Seguridad de la Información
Plan de Recuperación Ante Desastres (DRP): Responsable de la coordinación de las actividades en procura de la restauración eficaz de los sistemas y datos después de un desastre o ataque. Además de realizar la coordinación con las áreas para diseñar o crear un plan de continuidad del negocio (BCP) con lo cual se genere la planificación necesaria para la continuidad de la operación durante la incidencia o evento en la Dirección General de Sanidad Militar	I	C/A/R	R	C	C	A/C
Gobierno TI						
Fomentar la investigación, análisis y proyección de nuevas tecnologías, con el fin de asesorar y orientar a la institución en la aplicación de nuevas tecnologías	A/I	C/A/R	C	R	C	C
Presentar y asesorar proyectos de investigación tecnológica que se pretendan implementar en la Dirección General de Sanidad Militar y el Grupo de Tecnologías De La Información Y Las Comunicaciones (GRTIC) con el objetivo de cerrar brechas tecnológicas y de prestación de servicio en la entidad	A/I	C/A/R	C	R	C	C
Estudiar y analizar técnicamente los nuevos sistemas, tecnologías y aplicaciones, con el fin de determinar la viabilidad de incorporación y su respectiva alineación con el direccionamiento estratégico de la entidad para el fortalecimiento del servicio a los afiliados de la entidad	A/I	C/A/R	C	R	C	A/C
Asesorar a la Dirección General de Sanidad Militar y al Grupo de Tecnologías De La Información Y Las Comunicaciones (GRTIC) en cuanto a las prioridades en la consecución de nuevas tecnologías	A/I	C/A/R	C	R	C	C
Gobierno Digital: Definir, implementar, mantener y divulgar la arquitectura empresarial para la gestión de tecnologías de la información la Dirección General de	A/I	C/A/R	C	R	C	C/A

Funciones/Dependencias	Comité de Gestión y Desempeño	Coordinador SISAM	Equipo De Operaciones TIC	Equipo de Gobierno TI	Equipo De Gestión De Sistemas De Información Aplicaciones Y	Equipo de Gestión de la Seguridad de la Información
Sanidad Militar y al Grupo de Tecnologías De La Información Y Las Comunicaciones (GRTIC), en virtud de las definiciones y lineamientos establecidos en el marco de referencia de arquitectura empresarial del Estado emitido por el Ministerio TIC						
Desarrollar y actualizar las políticas, lineamientos y estrategias en materia tecnológica, en sistemas de información y en servicios digitales, con el fin de habilitar la gestión y gobernabilidad de las Tecnologías de la Información (TI) y la prestación efectiva de los servicios tecnológicos de la Dirección General de Sanidad Militar y al Grupo de Tecnologías De La Información Y Las Comunicaciones (GRTIC).	A/I	C/A/R	C	R	C	C/A
Analizar, diagnosticar, diseñar y desarrollar y/o Implementar herramientas que permitan mejorar la toma decisiones en la de la Dirección General de Sanidad Militar, para impulsar el desarrollo de servicios, políticas, normas, planes, programas, proyectos a partir del uso y aprovechamiento de datos que incorporan estándares de calidad y seguridad en su ciclo de vida (generación, recolección, almacenamiento, procesamiento, compartición, entrega, intercambio y eliminación).	A/I	C/A/R	C	R	C	C/A
Gobierno Digital: Definir, implementar, mantener y divulgar la arquitectura empresarial para la gestión de tecnologías de la información la Dirección General de Sanidad Militar y al Grupo de Tecnologías De La Información Y Las Comunicaciones (GRTIC), en virtud de las definiciones y lineamientos establecidos en el marco de referencia de arquitectura empresarial del Estado emitido por el Ministerio TIC.	A/I	C/A/R		R	C	C

Funciones/Dependencias	Comité de Gestión y Desempeño	Coordinador SISAM	Equipo De Operaciones TIC	Equipo de Gobierno TI	Equipo De Gestión De Sistemas De Información Aplicaciones Y	Equipo de Gestión de la Seguridad de la Información
Analizar, definir, actualizar y diseñar los planes y servicios TIC, como son el Plan Estratégico de Tecnologías de la Información – PETI y el plan de acción TIC	A/I	C/A/R	C	R	C	C
Desarrollar y actualizar las políticas, lineamientos y estrategias en materia tecnológica, en sistemas de información y en servicios digitales, con el fin de habilitar la gestión y gobernabilidad de las Tecnologías de la Información (TI) y la prestación efectiva de los servicios tecnológicos de la Dirección General de Sanidad Militar y al Grupo de Tecnologías De La Información Y Las Comunicaciones (GRTIC).	A/I	C/A/R	C	R	C	C
Analizar, diagnosticar, diseñar y desarrollar la provisión de Servicios Digitales de confianza y calidad, esto es, poner a disposición de ciudadanos, usuarios y grupos de interés, trámites y servicios de la Dirección General de Sanidad Militar que cuenten con esquemas de manejo seguro de la información, que estén alineados con la arquitectura institucional de la Dirección General de Sanidad Militar (Arquitectura misional y Arquitectura de TI) a fin de que éstos sean ágiles, sencillos y útiles para los usuarios	A/I	C/A/R	C	R	C	C
Mesa De Servicio: Encargado de la atención de incidentes y requerimientos, entendiendo que los requerimientos se enfocan en satisfacer las necesidades y expectativas de los usuarios, mientras que los incidentes se centran en la resolución de eventos no planificados que afectan la calidad del servicio; a los usuarios de la Dirección General de Sanidad Militar para garantizar la disponibilidad de la plataforma tecnológica	A/I	C/A/R	C	R	C	C
Gestión de Sistemas de Información Aplicaciones y Base De Datos						

Funciones/Dependencias	Comité de Gestión y Desempeño	Coordinador SISAM	Equipo De Operaciones TIC	Equipo de Gobierno TI	Equipo De Gestión De Sistemas De Información Aplicaciones Y	Equipo de Gestión de la Seguridad de la Información
Gestión, administración, seguridad, seguimiento, control y monitoreo de las bases de datos de la Dirección General de Sanidad Militar, adicionalmente deberá identificar posibles fallas o riesgo que pudieran generar la pérdida o no disponibilidad de la información de la entidad	I	C/A/R	C	C	R	C
Administrar las bases de datos y servidores relacionados con ellas de la Dirección General de Sanidad Militar, para garantizar el funcionamiento y la disponibilidad de la información	I	C/A/R	C	C	R	C
Estandarizar los procedimientos del Backup (Copias de Seguridad) y Dirigir y coordinar la integridad del respaldo de las bases de datos y de servidores relacionados con ellas, para garantizar la disponibilidad de la información	I	C/A/R	C	C	R	C
Documentar los procedimientos, modificaciones y estructura de las bases de datos y servidores relacionados con ellas del Grupo de Tecnologías De La Información Y Las Comunicaciones (GRTIC).	I/A	C/A/R	C	C	R	C
Gestión De Aplicaciones: Encargado de generar el soporte en el área de tecnología, permitiendo la operatividad continúa de las Aplicaciones Ofimáticas y Sistemas informáticos asignados que hacen parte del inventario de servicios y aplicaciones de la Dirección General de Sanidad Militar.	I	I	C	C	R	C
Administrar y controlar el desarrollo del plan de mantenimiento y soportes de las Aplicaciones Ofimáticas y Sistemas informáticos asignados que hacen parte del inventario de servicios y aplicaciones de la Dirección General de Sanidad Militar	I	I	I	C	R	C
Gestión De Sistemas De Información: Establecer y gestionar el cumplimiento de las políticas, lineamientos, metodologías, estándares y procedimientos	I	C/A/R	C	C	R	C

Funciones/Dependencias	Comité de Gestión y Desempeño	Coordinador SISAM	Equipo De Operaciones TIC	Equipo de Gobierno TI	Equipo De Gestión De Sistemas De Información Aplicaciones Y	Equipo de Gestión de la Seguridad de la Información
definidos por la Dirección General de Sanidad Militar y al Grupo de Tecnologías De La Información Y Las Comunicaciones (GRTIC) para el desarrollo y administración de los sistemas de información, fortaleciendo los sistemas de información para el mejoramiento de la operación y control de los procesos de la Entidad, aplicando los estándares y lineamientos definidos por el Ministerio TIC						
Orientar la gestión e intercambio de información que se requiera a nivel institucional y/o sectorial y/o transversal, acorde con las competencias de la entidad, flujos de información y los criterios de calidad, seguridad e interoperabilidad de la Dirección de Sanidad Militar	A/I	C/A/R	C	C	R	C
Gestión de la Seguridad de la Información						
Seguridad De La Información: Encargado de proteger los activos de información de la Dirección de Sanidad Militar la disponibilidad, confidencialidad e integridad de las tecnologías de la información	A/I	R	C	C	C	R/A
Diseñar, implementar y actualizar el manual de políticas de seguridad de la información de la Dirección de Sanidad Militar.	I	R	C	C	C	R/A
Elaborar, clasificar y analizar los riesgos de los activos de la información, a fin de aplicar controles para mitigar el riesgo en la Dirección de Sanidad Militar	I	R	C	C	C	R/A
Aplicar controles de seguridad de la información, para garantizar su confidencialidad, integridad y disponibilidad con el fin de minimizar el riesgo de pérdida, fuga o modificación de la información	I	R	C	C	C	R/A
Aplicar controles de seguridad de la información con el fin de proteger la integridad intelectual	I	R	C	C	C	R/A

Funciones/Dependencias	Comité de Gestión y Desempeño	Coordinador SISAM	Equipo De Operaciones TIC	Equipo de Gobierno TI	Equipo De Gestión De Sistemas De Información Aplicaciones Y	Equipo de Gestión de la Seguridad de la Información
Coordinar la realización de pruebas de vulnerabilidades a los sistemas de información que se pretendan implementar en la Dirección de Sanidad Militar.	I	R		C	C	R/A

Fuente: Elaboración propia SISAM

9.4. Gestión de Proyectos

Con el objetivo de Fortalecer el Proceso de Gestión de Proyectos de TI se realizará la revisión del Modelo de Gestión de Proyectos MGPTI, identificando los lineamientos de los cuatros dominios (Contexto Estratégico, Planeación, Ejecución y Control, Cierre y Operación), y priorizando aquellas actividades que permitan la implementación de este modelo al interior de la institución. El proceso seguirá aplicando la metodología descrita en la situación actual y dentro de la vigencia 2025 – 2026 se realizará los ajustes acordes la Modelo de Gestión de Proyectos MGPTI de los lineamientos priorizados.

9.5. Gestión de la información

Gestión de la información (GI) es la denominación convencional de un conjunto de procesos por los cuales se controla el ciclo de vida de la información, desde su obtención (por creación o captura), hasta su disposición final (su archivo o eliminación). Tales procesos también comprenden la extracción, combinación, depuración y distribución de la información a los interesados. El objetivo de la gestión de la información es garantizar la integridad, disponibilidad y confidencialidad de la información.

En el contexto de la Dirección General de Sanidad Militar (DIGSA), la gestión de la información se puede identificar como los procedimientos que se encargan de todo lo relacionado con la obtención de la información adecuada, en la forma correcta, para los funcionarios indicados, en el momento oportuno, en el lugar apropiado y articulando todas estas operaciones para el desarrollo de una acción correcta. En este contexto, los objetivos principales de la Gestión de la Información son: maximizar el valor y los beneficios derivados del uso de la información, minimizar el procesamiento y maximizar el uso de la información, determinar responsabilidades para el uso efectivo, eficiente y económico de la información y asegurar un suministro continuo de la información:

Ilustración 22. Gestión de la Información

La Dirección General de Sanidad Militar – DIGSA, dispone cada vez de más datos sobre sus operaciones diarias, sobre los cuales puede obtener información relevante para mejorar el desempeño e innovar en sus procesos de manera que se transforme en una organización que tome decisiones basadas en hechos e información inteligente. Esto se puede lograr mediante el diseño e implementación de un Modelo de Gobierno de Datos acorde a su estructura organizacional y necesidades.

La Inteligencia de Negocios para la DIGSA es necesaria, ya que constituye un apoyo importante a la toma de decisiones para los interesados internos y externos a la Dirección General de Sanidad Militar, sin embargo, esta solución debe coexistir con otros elementos o componentes que hacen parte de un Gobierno de Datos, como la Gestión de la Arquitectura de Datos, Bodegas de Datos, Inteligencia de Negocio y Analítica avanzada.

El diseño del Modelo de Gobierno de Datos para la DIGSA, de acuerdo con los resultados de la evaluación del estado de madurez de DIGSA en Gobierno de Datos, Arquitectura de Datos, Inteligencia de Negocios y Analítica, frente al marco de referencia DMBOK v2 del 2017, contempla fortalecer la definición, aplicación y monitoreo colaborativo de estrategias, principios, políticas, procesos, métricas, roles, responsabilidades y herramientas de soporte al Gobierno de Datos.

El Decreto 1078 de 2015 numeral 4 del artículo 2.2.9.1.2.1, *establece como uno de los elementos que componen la estructura de la Política de Gobierno Digital, la línea de acción denominada "Decisiones basadas en datos", la cual busca promover el desarrollo económico y social del país impulsado por datos, entendiéndolos como infraestructura y activos estratégicos, a través de mecanismos de gobernanza para el acceso, intercambio, reutilización y explotación de los datos, que den cumplimiento a las normas de protección y tratamiento de datos personales y permitan mejorar la toma de decisiones y la prestación de servicios de los sujetos obligados*.

El Decreto 1078 de 2015 en su artículo 2.2.9.1.2.1 manifiesta que la Política de Gobierno Digital se debe desarrollar a través de un esquema que articule los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción e iniciativas dinamizadoras, estableciendo el habilitador de Arquitectura, que tiene como objetivo que los sujetos obligados a implementar esta Política

desarrollen capacidades para el fortalecimiento institucional, implementando el enfoque de arquitectura empresarial en la gestión, gobierno y desarrollo de proyectos con componentes de Tecnologías de la información.

Igualmente, el artículo 148 de la Ley 1955 de 2019, establece, el gobierno digital como política de gestión y desempeño institucional, y como acción prioritaria para el cumplimiento de la política, el aprovechamiento de los datos públicos.

Por las razones expuestas mediante la Resolución 1267 de 2020, la Dirección General de Sanidad Militar adoptó el Modelo Integrado de Planeación y Gestión (MIPG), y en esta Resolución se asignó al Comité Institucional de Gestión y Desempeño funciones asociadas a la Política de Gobierno Digital.

A través de la Resolución 460 de 2022, el Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC) expidió el Plan Nacional de Infraestructura de Datos (PNID) y su Hoja de Ruta, con el fin de impulsar la transformación digital del Estado y el desarrollo de una economía basada en los datos, estableciendo los lineamientos generales para su implementación.

Mediante el decreto 1263 de 2022, el Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC) expidió los Lineamientos y Estándares para la Transformación Digital de la Administración Pública. En el Artículo 2.2.23.1.4. Lineamientos y Estándares para la Transformación Digital de la Administración Pública, ítem 4.1. Uso de la infraestructura de datos, dice: ” *Los sujetos obligados propenderán por el uso y aprovechamiento de la infraestructura de datos, dando cumplimiento al Plan Nacional de Infraestructura de Datos, la línea de acción de decisiones basadas en datos, el habilitador de seguridad y privacidad de la información y en general, todos los elementos que componen la Política de Gobierno Digital y sus lineamientos, guías y estándares, así como las normas en materia de tratamiento de datos personales*.” Que, con el Decreto 1389 de 2022, el Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC) expidió los lineamientos generales para fortalecer la gobernanza de infraestructura de datos y crear el Modelo de Gobernanza de la Infraestructura de Datos., estableciendo instancias y roles específicos por medio del relacionamiento de actores del ecosistema digital, lo cual resulta fundamental para crear valor público y fomentar la competitividad del país a través del uso y aprovechamiento de los datos.

El Decreto 1389 de 2022, define el Modelo de Gobernanza de la Infraestructura de Datos como “el conjunto de elementos políticos, técnicos, legales y organizacionales que permiten la articulación de actores, instancias, normas, políticas, planes, programas, estrategias, metodologías, compromisos, procesos y procedimientos para implementar, fortalecer, gestionar y manejar la infraestructura de datos, con la finalidad de generar valor público, social y económico, a través de los datos, teniendo como objetivos:

1. Definir los actores, instancias, normas, políticas, planes y proyectos, para implementar, fortalecer, gestionar y dar sostenibilidad a la infraestructura de datos.
2. Promover el entendimiento común de los datos bajo el concepto de infraestructura.
3. Facilitar la coordinación interinstitucional entre las múltiples partes interesadas, incluidos representantes del sector público, sector privado, academia y organizaciones de la sociedad civil.
4. Fortalecer las capacidades técnicas, humanas y administrativas de los distintos actores para la adopción de enfoques comunes en materia de datos.
5. Articular esfuerzos interinstitucionales para la implementación y actualización de la hoja de ruta del Plan Nacional de Infraestructura de Datos, o la que haga sus veces, en torno a las competencias y capacidades de cada actor.

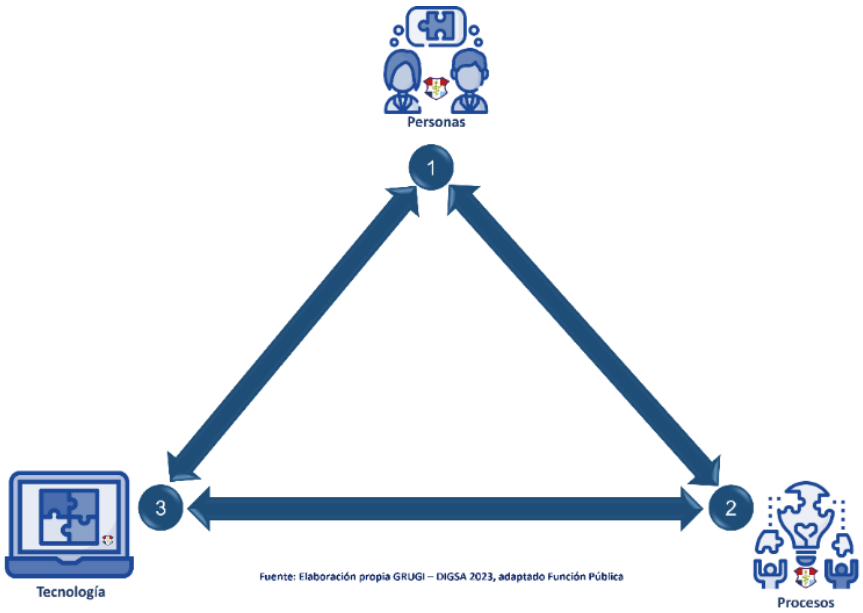
9.5.1. Planeación y Gobierno de la Gestión de Información

La arquitectura de la información es el arte de organizar la información de la forma más clara y lógica posible. De este modo, el usuario podrá encontrar fácilmente lo que está buscando. Además, también nos permitirá poder añadir fácilmente nuevas funcionalidades y escalar el producto de forma eficiente sin que acabe generando una arquitectura que sea difícil o imposible comprender.

Podemos hacer una analogía con la construcción: para poder tener un buen bloque de pisos necesitamos un arquitecto y que los cimientos estén bien hechos, con una buena base. Si no lo están, a la larga aparecerán grietas y el edificio puede llegar a derrumbarse.

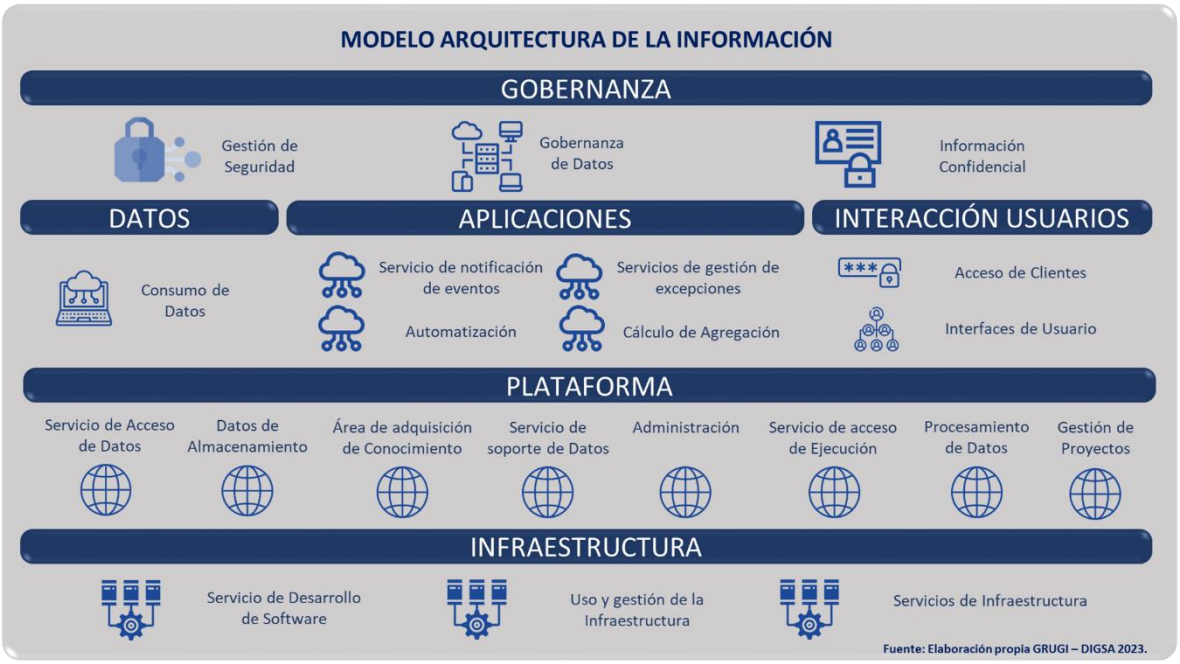
Con un producto digital pasará lo mismo: si no hay caminos bien definidos vamos a generar inconsistencias e incoherencias, el usuario se perderá y es muy posible que no vuelva (y, además, difícilmente conseguiremos nuestros objetivos, sean estos vender, conseguir suscriptores o ganar notoriedad).

Según Morville, estos son los tres pilares sobre los que se sustenta la arquitectura de la información:



El modelo planteado para la Dirección General de Sanidad Militar es:

Ilustración 23. Modelo MAE



9.5.2. Planeación y Gobierno de la Gestión de Información

La Dirección General de Sanidad Militar en cumplimiento de la política de Gobierno Digital y la Guía G. INF. 06 Guía Técnica de Información – Gobierno de Datos elaborado por Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, elabora los lineamientos para la administración y gestión de los diferentes componentes de información que orienten a la Entidad sobre la forma de implementar, mantener y mejorar un programa de Gobierno de Datos, con el fin de aportar al avance en la madurez en la gestión de datos, priorizando los datos maestros a gobernar según el flujo de información presente en diferentes procesos y procedimientos.

Bajo estos lineamientos es necesario reconocer la evolución que presentan los datos para convertirse en activos de valor y generar propósitos concretos que avalen la tome de decisiones en todos niveles jerárquicos de las instituciones no solo del gobierno sino también de las empresas privadas que apoyan el crecimiento del país.

Por otro lado, este documento incluye conceptos y definiciones basado en las mejores prácticas recogidas del DAMA-DMBOK2 y lineamientos del MinTic, para garantizar la calidad de los datos a lo largo de su ciclo de vida, como activo principal y transversal de los procesos internos.

Igualmente, se incluye conceptos y parámetros del Diseño del Gobierno de Datos, arquitectura de datos e inteligencia de negocios y analítica con base en DMBOK versión 1 de 2023, producto de la consultoría para la definición y diseño del Modelo de Gobierno de Datos de la Dirección General de Sanidad Militar (DIGSA).

El gobierno de datos fija los estándares internos (es decir, políticas de datos) que regulan cómo se recopilan, almacenan, procesan y eliminan los datos. Rige quiénes pueden acceder a qué tipos de datos y cuáles de estos están sometidos al gobierno. También implica cumplir los estándares externos que fijan los entes de control, los organismos públicos y otras partes interesadas. Además, es garantía para los procesos de transformación descritos a continuación:

- Eficiencia operativa (valor para TI): flujos de datos más eficientes, menos incidencias y rechazos por calidad de datos; trazabilidad, reutilización de componentes, robustez de las soluciones y rendimiento.
- Conocimiento del dato (valor para la función pública): visión integrada y unificada 360º del ciudadano y grupos de interés, campañas mejor orientadas, convergencia, control de datos sensibles y coherencia de datos.
- Uso de información (valor en la transformación): se refiere al uso de información de calidad en los procesos o iniciativas de migración / fusión de datos hacía una institución convergente, multicanal y con una oferta simplificada. Facilitando con esto la gestión de la transformación y el proceso de migración de datos.

Como base fundamental del Gobierno del Dato es optar por seguir una gestión adecuada en los siguientes ámbitos:

Ilustración 24. Ámbitos Gobierno de Datos

Fuente: Elaboración propia GRUGI – DIGSA 2023, adaptado MINTIC

9.5.3. Gestión de la calidad y seguridad de la información

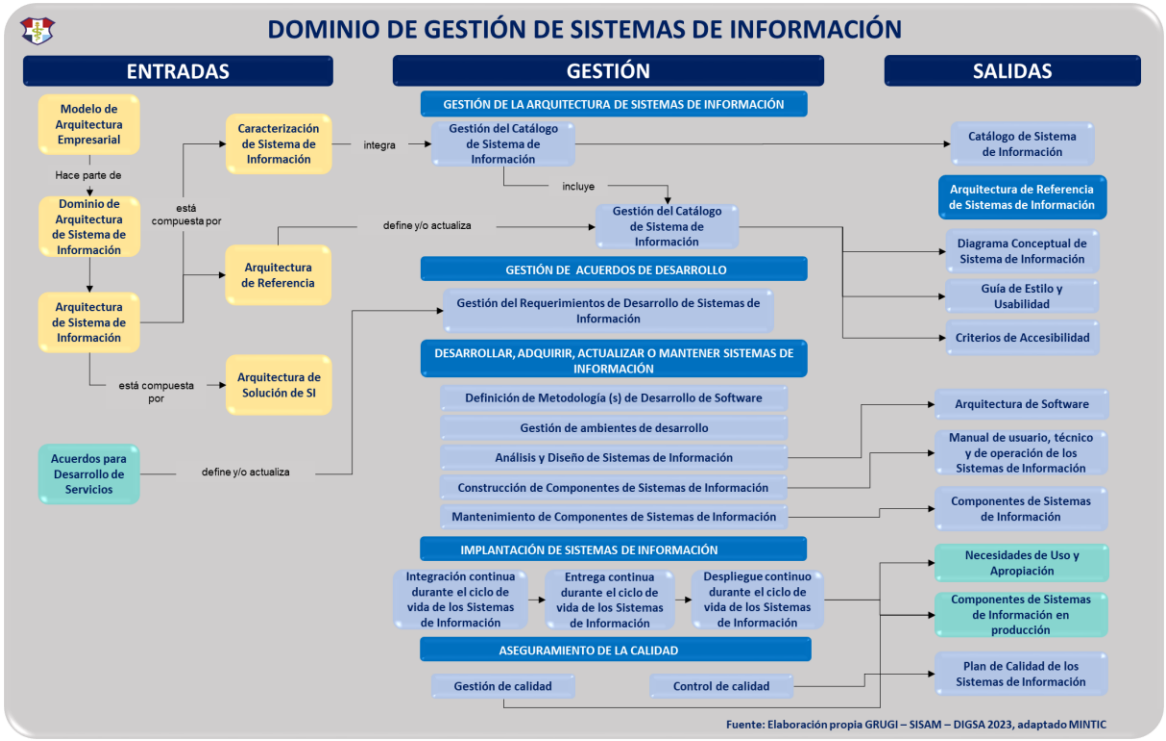
El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios de la Dirección General de Sanidad Militar, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital.

9.5.4. Análisis y aprovechamiento de la información

El análisis de datos es el proceso de exploración, transformación y examinación de datos para identificar tendencias y patrones que revelen insights importantes y aumenten la eficiencia para respaldar la toma de decisiones.

La Dirección General de Sanidad Militar está revisando la estrategia de análisis de datos, a partir del modelo de la Gestión de Sistemas de Información, para trabajar a partir de análisis automatizados en tiempo real, lo que garantiza resultados inmediatos y de gran impacto, en las salidas el modelo contempla las necesidades de uso y apropiación de la información:

Ilustración 25. Gestión de la calidad y seguridad de la información



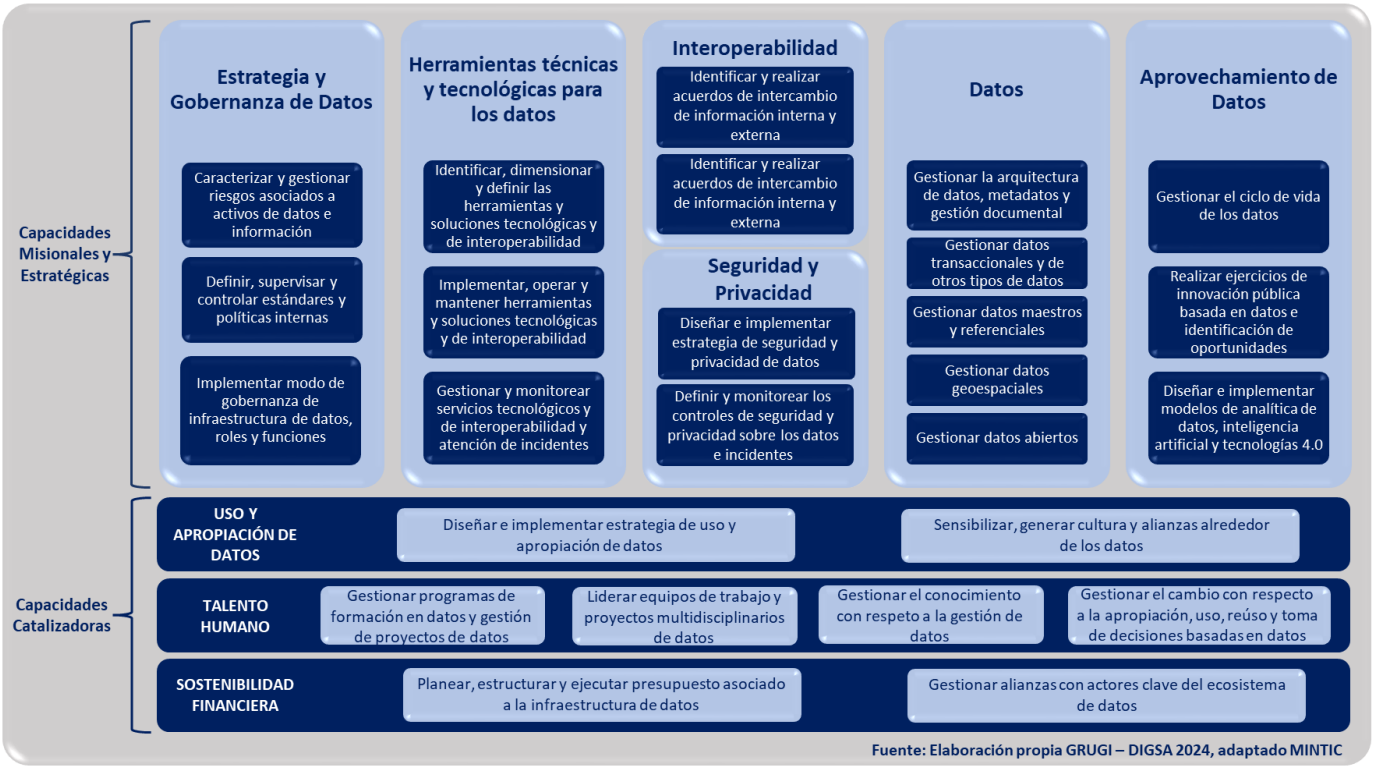
Fuente: Elaboración propia GRUGI

9.5.5. Desarrollo de capacidades para el uso de la información

En el contexto de la infraestructura de Datos para el estado, una capacidad puede definirse como una habilidad o conjunto de habilidades específicas que la Dirección General de Sanidad Militar debe desarrollar para lograr un propósito o resultado específico relacionado con la implementación y gestión efectiva de la infraestructura de datos.

En este sentido, una capacidad se expresa mediante un verbo que indica lo que una entidad o empresa debe desarrollar o fortalecer, sin profundizar en cómo, por qué o dónde se aplicará esa habilidad. En otras palabras, la habilidad se centra en la "acción" o "tarea" que la entidad puede llevar a cabo en el contexto de la infraestructura de datos, sin entrar en los detalles operativos. Para proporcionar un marco general que permita comprender las acciones necesarias, se ha elaborado un mapa de capacidades que se presenta a continuación. En este mapa de capacidades, se distinguen las habilidades denominadas "Capacidades de Nivel 1" y los paquetes que las agrupan:

Ilustración 26. Desarrollo de capacidades para el uso de la información



Fuente: Elaboración propia GRUGI

9.6. Sistemas de Información

Dentro de este dominio se proyecta disponer de un Sistema de Información Integrado que permita la gestión eficiente y unificada de la información en toda la institución. Este objetivo busca superar la fragmentación y la falta de cohesión entre los sistemas de información existentes, facilitando así la toma de decisiones informadas y la mejora de los procesos operativos y administrativos, a continuación, se enmarcan las acciones claves para el cumplimiento de esta actividad:

- Evaluación de Plataformas Tecnológicas y de Software Actuales de la DIGSA: Realizar un análisis exhaustivo de las plataformas Tecnológicas y de Software actualmente en uso en la DIGSA para identificar sus capacidades, limitaciones y áreas de mejora en términos de operación administrativa, integración e interoperabilidad.

- Identificación de Requerimientos de Integración y Gestión de Información Administrativa y Operativa: Determinar los requisitos específicos de Integración y Gestión de Información Administrativa y Operativa, gestión y explotación de datos y mejoramiento de procesos entre las diferentes plataformas tecnológicas y de software de la DIGSA, con el fin de garantizar una comunicación fluida y eficiente entre ellas.

- Implementación de Soluciones de Hardware y Software de Integración y Gestión de Información Administrativa y Operativa: Desarrollar e implementar las soluciones seleccionadas de Integración y Gestión de Información Administrativa y Operativa en la DIGSA, asegurando una integración adecuada y sin problemas con las plataformas existentes.

- Pruebas y Ajustes: Realizar pruebas exhaustivas de las soluciones de las diferentes herramientas de Integración y Gestión de Información Administrativa y Operativa implementadas para verificar su funcionalidad, rendimiento y compatibilidad con las plataformas existentes, y realizar los ajustes necesarios para garantizar su correcto funcionamiento.

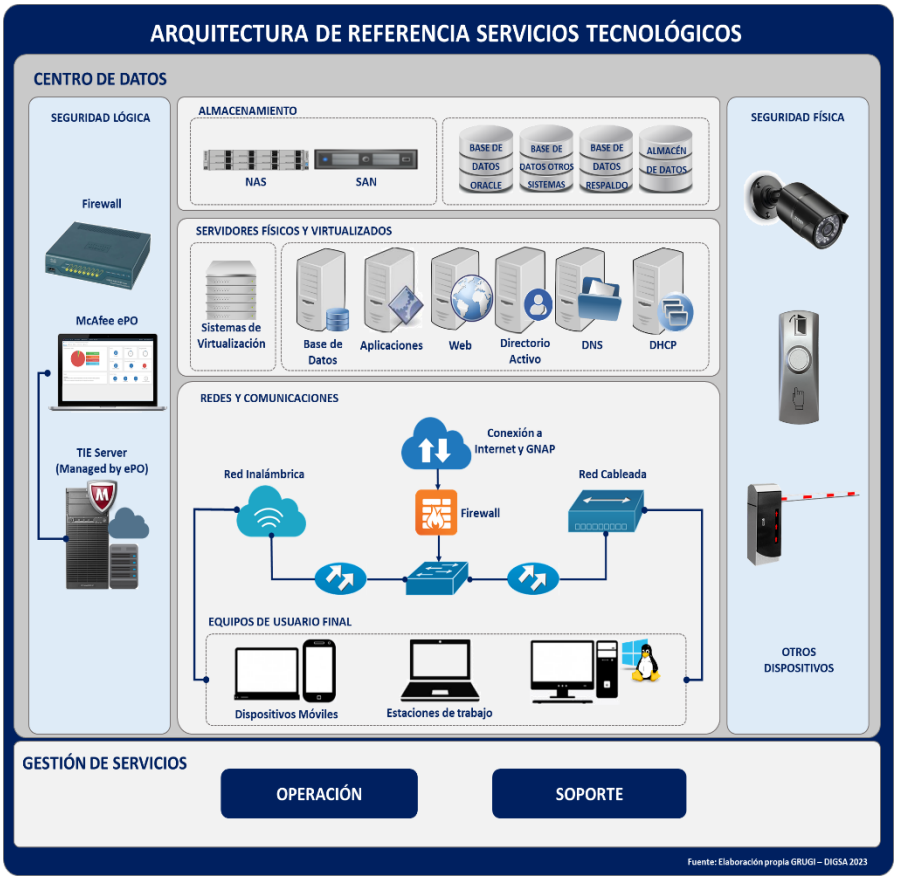
- Capacitación del Personal: Capacitar al personal de la DIGSA en el uso y la administración de las nuevas soluciones de Integración y Gestión de Información Administrativa y Operativa, asegurando que estén familiarizados con sus características y puedan aprovechar al máximo sus capacidades.

Al lograr este objetivo, la DIGSA podrá contar con un sistema de información integrado que mejore la eficiencia operativa, facilite la toma de decisiones basadas en datos y promueva una atención médica de calidad para las Fuerzas Militares y sus familias. Este sistema integrado servirá como una herramienta fundamental para la modernización tecnológica de la institución y su adaptación a los desafíos y oportunidades del entorno de salud actual.

9.6.1. 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 27. Arquitectura de Referencia



Fuente: Elaboración propia GRUGI

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.

9.6.2. Ciclo de Vida de los Sistemas de Información

Tabla 40. Ciclo de Vida de los Sistemas de Información

Actividad	Grado de Madurez (Optimizado, Implementado Informal, No tiene, No aplica	Descripción del Hallazgo u Oportunidad de Mejora	Acción de Mejora
Levantamiento de Necesidades de Sistemas de Información	Implementado Para cambios en el Sistema Información SALUD.SIS se tiene implementado el formato de solicitud de requerimientos donde se establecen los criterios de solicitud, propuesta y validación, Prioridad, Descripción de la Solicitud (Requerimiento, Para que, Dado Que, Cuando, Entonces y Evidencias, Anexos).	Los líderes funcionales tengan el contexto generalizado de las solicitud, propuestas y validación del requerimiento. Que existe un funcionario Operativo de SALUD.SIS y no depender de un Contrato.	La Directiva Permanente No. 0124011306602/ MDN-COGFM-JEMCO-DIGSA-SUBTG-SISAM de octubre de 2024 definió lineamientos para definir el esquema de control y seguimiento en las actividades de soporte, mantenimiento y evolución del sistema de información SALUD.SIS del Subsistema de Salud de las Fuerzas Militares, como herramienta articuladora en la prestación de servicios de salud, con generación de datos para el análisis en la toma de decisiones a nivel estratégico
Análisis de requisitos funcionales y no funcionales	Implementado Validación en conjunto con el Gerente del Proyecto, Enlace Funcional, el Funcional y el Equipo de Soporte, de la Solicitud, Propuesta y Validación requerido en el Formato Solicitud de Requerimiento SALUD.SIS y Tecnologías de la Información. Aprobada la validación de la propuesta se realizada comunicación con enlace funcional, Gerente del Proyecto, supervisor del contrato para inicio del Diseño de la Solución.	Establecer un Procedimiento y/o lineamientos que permita estructurar equipo Táctico, Operativo - Funcional. Emitir lineamientos para definir el esquema de control y seguimiento en las actividades de soporte, mantenimiento y evolución del sistema de información.	Conformación de un Equipo Táctico y un Equipo Funcional - Operativo del Sistema de Información SALUD.SIS que permita la mejora continua del sistema de información Levantamiento del Procedimiento y formatos de registro.
	Implementado	Ajustar formato de requerimiento Formato Solicitud de	Revisar formato de requerimientos y ajustar de acuerdo con el

Actividad	Grado de Madurez (Optimizado, Implementado Informal, No tiene, No aplica	Descripción del Hallazgo u Oportunidad de Mejora	Acción de Mejora
Diseño de la solución	Se realiza refinamiento de la Historia de Usuarios. Mesas de Trabajo con los Funcionales, enlace funcional, gerente de proyecto, transversales al requerimiento para levantamiento de Historia de Usuarios.	Requerimiento SALUD.SIS y Tecnologías de la Información incorporando Análisis de Impacto/Urgencia y Matriz de Riesgos, implementar formato plan de pruebas.	Procedimiento de Control de Cambios.
Codificación del software	Implementado Proveedor (Contratista) inicia desarrollo de acuerdo con la solicitud de requerimiento con la propuesta y validación. Mesas de trabajo Gerente del Proyecto, Enlace Funcional, el Funcional y el Equipo de Soporte, cuando se presenten observaciones.		Levantamiento del Procedimiento y formatos de registro.
Aseguramiento de la calidad (pruebas)	Utilización de Ambiente de Pruebas, funcional, equipo de soporte, Gerente de Proyecto y Proveedores. Utilización de Ambiente de preproducción validado por el funcional, enlace funcional y Gerente de Proyecto, para despliegue de producción.	Ajustar formato de requerimiento Formato Solicitud de Requerimiento SALUD.SIS y Tecnologías de la Información alineado al formato de pruebas del Sistemas de Información.	Levantamiento del Procedimiento y formatos de registro.
Despliegue en Producción	Programación de Ventana de Mantenimiento de acuerdo a al impacto de usuarios y requerimiento.	Ajustar formato de requerimiento Formato Solicitud de Requerimiento SALUD.SIS y Tecnologías de la Información, incorporando Plan de Ejecución y Plan de Reversión (Roll-Back).	Levantamiento del Procedimiento y formatos de registro.

Fuente: Elaboración propia SISAM

9.7. 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.

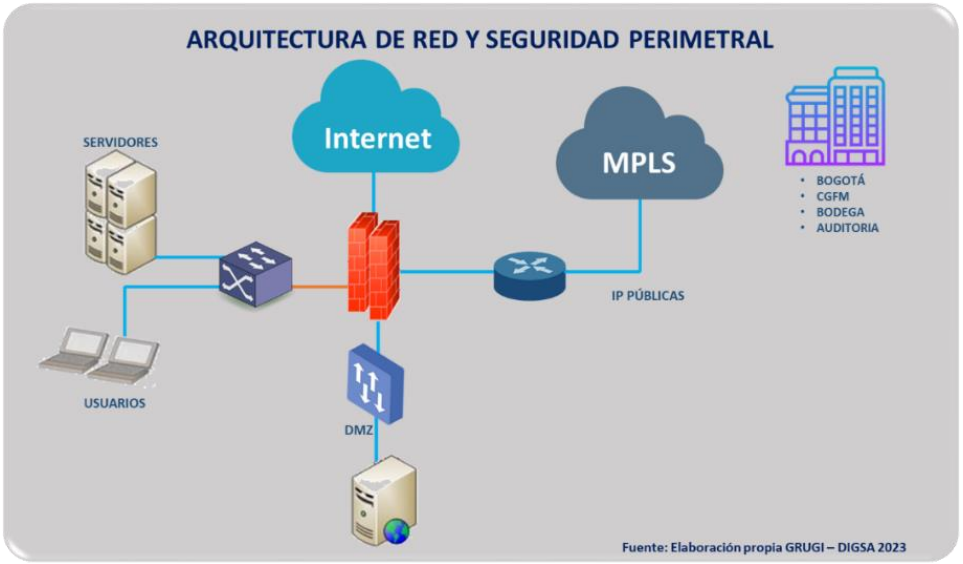
En la actualidad se cuenta con equipos de hiperconvergencia para manejar la administración de la infraestructura de TIC, a la fecha se han tenido entre otros los siguientes beneficios: Eficiencia de datos, movilidad, Escalabilidad y eficiencia, protección de datos, alta disponibilidad, eficiencia de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

9.7.1. 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 28. Arquitectura de Infraestructura tecnológica



Con el objetivo de disponer de una Infraestructura robusta que garantice la continuidad de los servicios tecnológico y mejorar el acceso a los servicios de los usuarios del SSFM, se proponen las siguientes actividades que son parte del proyecto de inversión que se proyectó como inversión que se proyecta y que se describirá en el capítulo de Portafolio de iniciativas, Proyectos y Mapa de Ruta del presente plan.

- Optimización de la Infraestructura Tecnológica: Actualizar y mejorar la infraestructura tecnológica de DIGSA, incluyendo hardware, software, redes y sistemas de comunicación, para garantizar un rendimiento óptimo y una disponibilidad continua de los servicios tecnológicos.

- Implementación de Mejores Prácticas: Incorporar mejores prácticas de gestión de servicios de tecnología de la información (TI), como la adopción de estándares de calidad (por ejemplo, ITIL) y la implementación de procesos de gestión de incidencias, problemas y cambios.

- Incremento de la Disponibilidad y Accesibilidad: Asegurar que los servicios tecnológicos de DIGSA estén disponibles y accesibles en todo momento, proporcionando una experiencia de usuario sin interrupciones y facilitando el acceso a la información y herramientas necesarias para el desempeño de las funciones.

- Mejora de la Experiencia del Usuario: Implementar interfaces de usuario intuitivas y amigables, así como procesos simplificados, que mejoren la experiencia del usuario al interactuar con los servicios tecnológicos de DIGSA.

- Monitoreo y Mejora Continua: Establecer mecanismos de monitoreo y evaluación para supervisar el rendimiento de los servicios tecnológicos, recopilar retroalimentación de los usuarios y realizar mejoras continuas en función de los comentarios recibidos y los resultados obtenidos.

9.8. Uso y Apropiación

9.8.1. Estrategia de Uso y Apropiación

Considerando que, en la Dirección General de sanidad Militar, se está planeado para la siguiente vigencia, iniciar la actualización del Modelo de Gestión y Gobierno de TI (MGGTI), teniendo en cuenta que el desarrollo e implementación de los dominós generan servicios y soluciones que van a generar valor a la entidad en la medida en que sean efectivamente usados e incorporados en los procesos y la cultura organizacional, resaltando la importancia del Dominio de Uso y apropiación de TI:

Ilustración 29. Modelo de Gestión y Gobierno de TI - MGGTI

Las entradas de este dominio son las necesidades de uso y apropiación de los componentes y soluciones de TI. El dominio de uso y apropiación de TI define y desarrolla acciones para movilizar a los grupos de interés para lograr usar y apropiar los diferentes componentes de TI con que cuenta la entidad y gestionar el cambio. Estas acciones se desarrollarán en tres bloques:

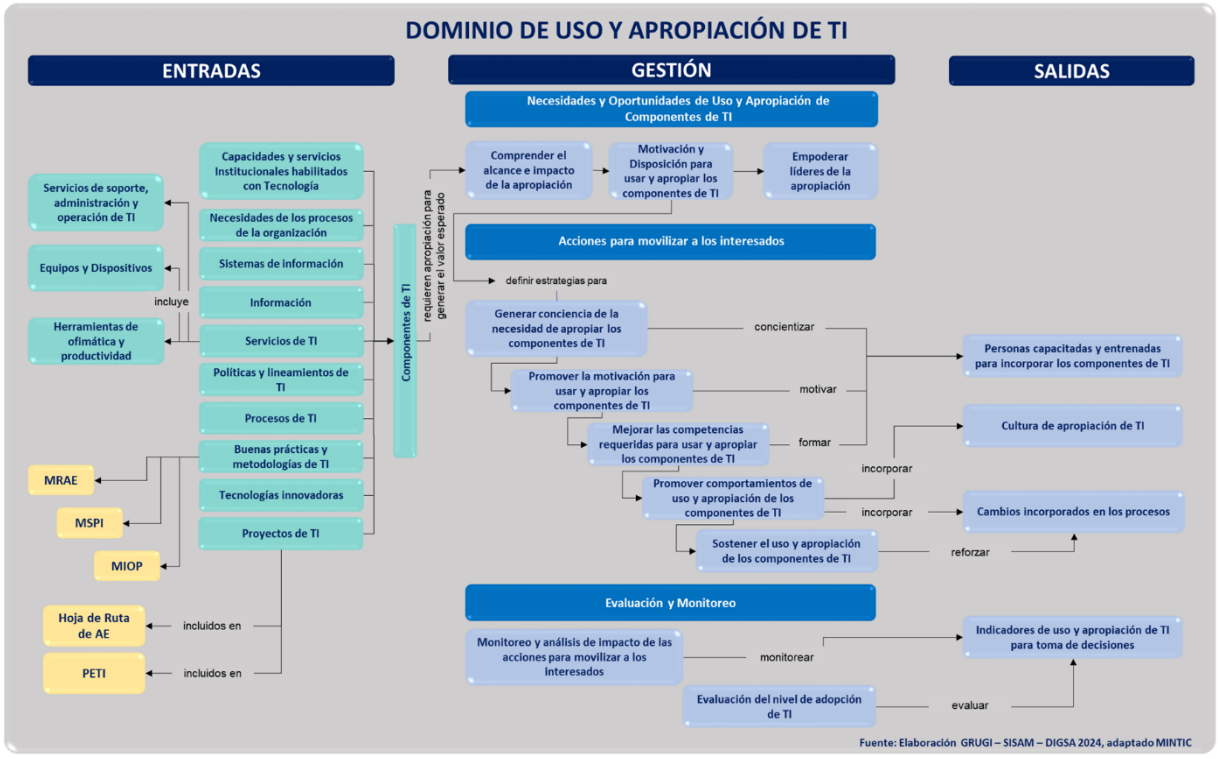
- El primero contextualiza las necesidades y oportunidades de uso y apropiación de componentes de TI, en este bloque se identifican las características de los interesados o el público objetivo, se establecen cuáles son los motivadores y la disposición de estos interesados para usar y apropiar los componentes de TI y se empoderan a los líderes de la iniciativa de apropiación.
- A partir de los hallazgos del bloque anterior, se desarrollará el segundo bloque en el cual se define las acciones para movilizar a los interesados o grupos de interés; estas acciones están dirigidas a cinco (5) propósitos específicos:

    1. Generar conciencia de la necesidad de la apropiación del componente de TI.
    2. Promover la motivación (inclusive atender las objeciones) para usar y apropiar los componentes de TI.
    3. Generar las competencias requeridas para estar en capacidad de usar y apropiar los componentes de TI.
    4. Promover los comportamientos que va a asegurar que el uso y apropiación de los componentes de TI se van a incorporar en las prácticas cotidianas durante la ejecución de los diferentes procesos.
    5. Sostener el uso y apropiación logrando una cultura organizacional de apropiación de TI.

- Finamente, el tercer bloque, constituye las actividades orientadas a evaluar y monitorear estas acciones, con el propósito de verificar constantemente si se están ejecutando de acuerdo con lo planeado, si es necesario realizar ajustes y finalmente si están teniendo el impacto deseado.

Modelo propuesto Dominio de Uso y apropiación de TI DIGSA:

Ilustración 30. Dominio de Uso y Apropiación de TI



Para el modelo se deben definir los componentes:

- Estrategia del uso y apropiación.
- Gestión del Cambio para el Uso y Apropiación.
- Medición de resultados del Uso y Apropiación.

9.9. 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 31. Modelo Seguridad y Privacidad de la Información

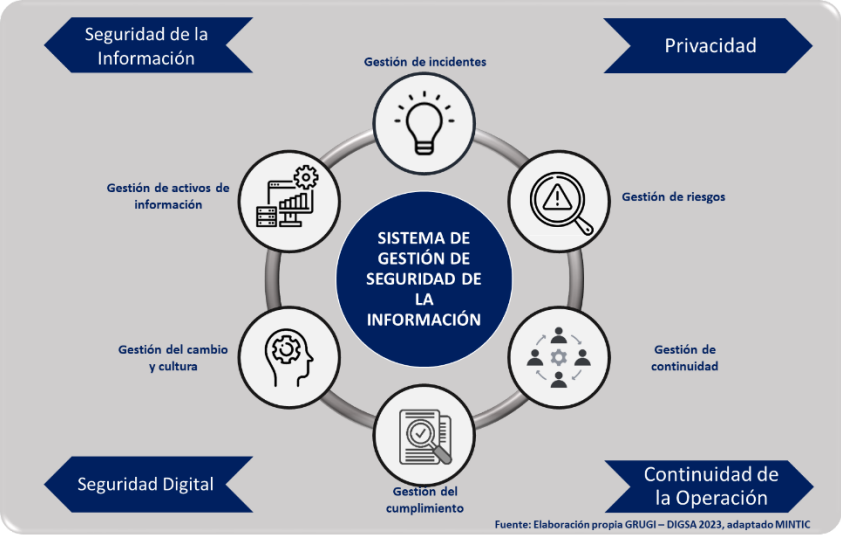
9.9.1. Sistema de Gestión de la Seguridad de la Información (SGSI)

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 32. Sistema de Gestión de Seguridad de la Información



10. Identificación de Hallazgos y Brechas

10.1. Falta De Integración en los Sistemas De Información

Define la necesidad de fortalecer la colaboración del Sistema de Información de la DIGSA entre las diferentes áreas internas y con entidades externas; entiéndase como sistema de información a todas las herramientas de software que utiliza la DIGSA para proveer los servicios de salud y la gestión administrativa interna de la entidad. Se busca mejorar la coordinación, la integración de sistemas y establecer alianzas estratégicas para abordar desafíos comunes y optimizar la satisfacción del usuario y por, sobre todo, aprovechar los datos que han venido acopiándose en años de servicios que ha prestado la DIGSA.

Ejes de Atención del problema

Falta de Colaboración Institucional

- Debilidad en la colaboración mediante coordinación efectiva y mejora de los
- Sistemas de Información.
- Debilidad en la Articulación institucional.
- Debilidad en la comunicación transparente.

Falta de Integración entre Dependencias

- No se considera la integración del enfoque empresarial con otras dependencias.
- No se visibiliza coordinación con el Grupo Sistema Integral de la Información Tecnologías de la Información y las Comunicaciones de la Dirección General de Sanidad Militar (DIGSA) para garantizar una integración eficiente.

No hay Colaboración con Entidades Externas

- No existe colaboración con entidades externas.
- No existe interoperabilidades y cumplimiento de estándares

Tomar Información de Otras Fuentes de Datos

- No existe la posibilidad de obtención de datos de otras fuentes para enriquecer la información de la DIGSA.

Gobernanza de Datos

- No existe capacidades de generación de datos para obtener información más precisa y relevante.
- No hay un marco de gobernanza de datos claro y eficiente para asegurar la calidad y consistencia de la información.

Calidad de Datos

- No se observa un plan de mejora integral de la calidad de la información, incluyendo validación de datos, depuración y control de calidad.
- No se observa una estrategia específica para mejorar la calidad de datos.
- No se observa una estrategia que permita abordar problemas de calidad y completitud de datos.

Análisis Avanzado y Tecnológico

- Mejorar la integración de datos para facilitar informes unificados. Resaltar la importancia del análisis de datos, la minería de datos y la inteligencia artificial.

Decisiones Informadas

- No hay interiorización de la importancia de tomar decisiones informadas basadas en datos de sistemas de información.
- Necesidad de generar indicadores basados en la información recolectada para focalizar la prestación de los servicios y la asignación de recursos para ello. Definir el tipo de información que pueda ser pública y refleje la realidad del servicio y del sector.
- Necesidad de Evaluar y mejorar las herramientas de análisis, incorporando capacidades avanzadas y proporcionando capacitación efectiva.
- Necesidad de identificar y caracterizar los grupos sociales objetivo de la DIGSA que permitan focalizar acciones en procura de mejorar su calidad de vida.

Comunicación y Colaboración

- No se observa un plan de comunicación de la DIGSA y todos sus grupos sociales objetivo que utilicen herramientas de presencia en la WEB y en dispositivos móviles.
- No se observan mecanismos y/o elementos que faciliten la auto atención de los grupos sociales objetivo en procura de mejorar la calidad de vida de estos.

10.2. Obsolescencia De Herramientas De Tecnología De La Información

En el contexto de un mundo cada vez más digitalizado, la Dirección General de Sanidad Militar (DIGSA) enfrenta el desafío crítico de mantenerse al día con los avances tecnológicos para continuar cumpliendo eficazmente con su misión de brindar atención médica de calidad a las Fuerzas Militares y sus familias. En este análisis para el desarrollo del proyecto de inversión de modernización tecnológica de la DIGSA, se ha identificado la obsolescencia de herramientas de tecnología de la información como un problema central que requiere una atención inmediata y estratégica.

La obsolescencia de las herramientas de tecnología de la información dentro de la DIGSA representa una barrera significativa para la eficiencia operativa y la prestación de servicios de salud de calidad. Este problema se manifiesta en varios aspectos críticos:

- Rendimiento y Fiabilidad: Las herramientas obsoletas suelen experimentar problemas de rendimiento y fiabilidad, lo que resulta en interrupciones del servicio, tiempos de inactividad prolongados y pérdida de datos. Esto no solo afecta la productividad del personal de salud, sino que también pone en riesgo la seguridad y la integridad de la información médica sensible.

- Compatibilidad e Interoperabilidad: La obsolescencia de las herramientas de tecnología de la información puede dificultar su compatibilidad con sistemas más nuevos y su capacidad para interoperar con otras plataformas y aplicaciones. Esto puede crear silos de información y obstaculizar la comunicación y la colaboración entre diferentes áreas y procesos dentro de la Entidad.

- Costos Operativos Elevados: Mantener y operar herramientas obsoletas conlleva costos operativos significativos, tanto en términos de mantenimiento regular como de reparaciones urgentes. Además, la falta de soporte técnico y actualizaciones de software puede resultar en costos aún mayores a largo plazo debido a la necesidad de reemplazar sistemas completos.

- Limitaciones en la Innovación: La obsolescencia tecnológica puede limitar la capacidad de la DIGSA para adoptar nuevas tecnologías y aprovechar innovaciones que podrían mejorar la eficiencia, la calidad y la accesibilidad de los servicios de salud. Esto coloca a la institución en desventaja competitiva y obstaculiza su capacidad para adaptarse a las demandas y necesidades cambiantes del entorno de salud.

10.3. Debilidad en el Conocimiento en Tecnologías De La Información

En el análisis para el desarrollo del proyecto de inversión de modernización tecnológica de la Dirección General de Sanidad Militar (DIGSA), la identificación de la "debilidad en el conocimiento en tecnologías de la información" se erige como un factor crucial que merece una atención prioritaria. Esta identificación se justifica por diversas razones que reflejan los desafíos inherentes a la falta de capacitación y experiencia en tecnología dentro de la Entidad:

- Escasa Capacitación Especializada: La debilidad en el conocimiento en tecnologías de la información puede atribuirse a la falta de capacitación especializada del personal de la DIGSA en áreas relevantes como ciberseguridad, infraestructura, gestión de datos, desarrollo de software y sistemas informáticos. Esta falta de capacitación puede limitar la capacidad del personal para aprovechar plenamente el potencial de las herramientas tecnológicas disponibles y para adaptarse a las nuevas innovaciones.

- Riesgos en Seguridad de la Información: La falta de conocimiento en tecnologías de la información puede exponer a la DIGSA a riesgos significativos en cuanto a seguridad de la información, como brechas de seguridad, ciberataques y violaciones de privacidad de datos. La falta de comprensión sobre las mejores prácticas de seguridad cibernética y la gestión adecuada de datos sensibles puede poner en peligro la integridad y confidencialidad de la información médica de los usuarios de la DIGSA.

- Limitaciones en la Adopción de Nuevas Tecnologías: La debilidad en el conocimiento en tecnologías de la información puede obstaculizar la capacidad de la DIGSA para adoptar nuevas tecnologías y aprovechar las innovaciones que podrían mejorar la eficiencia y calidad de los servicios de salud. La falta de comprensión sobre el potencial y las aplicaciones de nuevas herramientas tecnológicas puede generar resistencia al cambio y dificultar la implementación de mejoras tecnológicas.

- Dificultades en la Gestión de Proyectos Tecnológicos: La falta de conocimiento en tecnologías de la información puede afectar la capacidad de la DIGSA para gestionar eficazmente proyectos tecnológicos complejos. La falta de experiencia en la planificación, implementación y evaluación de

proyectos tecnológicos puede resultar en retrasos, presupuestos desviados y resultados insatisfactorios.

- La identificación de la debilidad en el conocimiento en tecnologías de la información destaca la necesidad crítica de fortalecer las capacidades técnicas y profesionales del personal de la DIGSA en el ámbito de la tecnología. Abordar esta debilidad requerirá una inversión significativa en programas de capacitación y desarrollo profesional, así como una cultura organizacional que fomente el aprendizaje continuo y la actualización de conocimientos. Solo a través de estos esfuerzos podrá la DIGSA maximizar el potencial de su modernización tecnológica y garantizar una prestación de servicios de salud de calidad y seguridad.

10.4. Ejes de Atención del Problema:

- Capacitación y Usabilidad: No se observa una fusión de iniciativas de capacitación y formación con mejoras en la usabilidad de los sistemas de la DIGSA.
- Aprendizaje Continuo: No se observa una documentación formal de lecciones aprendidas.
- Capacitación y Acceso a Información: No se observa una implementación de un programa integral de capacitación que abarque aspectos de administración, gestión y operación de las diferentes infraestructuras y servicios tecnológicos de la DIGSA.
- Mejora Continua y Capacitación: No se observa una Implementación de procesos de mejora continua, asistencia técnica, y capacitación constante para los usuarios.
- Retención de Conocimiento: No se observa un establecimiento de una cultura de mejora continua mediante mecanismos de feedback. Ni se identifica el fomento de la retención del conocimiento a través de documentación detallada de procesos y capacitación continua.

10.4.1. Deficiencia en los Mecanismos de Continuidad del Negocio Administrativo y/u Operativo

En el análisis exhaustivo llevado a cabo para el desarrollo del proyecto de inversión en modernización tecnológica de la Dirección General de Sanidad Militar (DIGSA), se ha identificado la "deficiencia en los mecanismos de continuidad del negocio administrativo y/o operativo" como un problema crítico que requiere una atención inmediata. Esta identificación se justifica por una serie de razones fundamentales que subrayan los riesgos y desafíos asociados con la falta de una planificación adecuada para garantizar la continuidad de las operaciones:

- Vulnerabilidad ante Interrupciones: La ausencia de mecanismos robustos de continuidad del negocio deja a la DIGSA vulnerable ante posibles interrupciones en sus operaciones, ya sean causadas por desastres naturales, fallas tecnológicas, ataques cibernéticos u otros eventos imprevistos. Esta vulnerabilidad puede tener un impacto significativo en la capacidad de la institución para brindar servicios de salud de manera ininterrumpida a las Fuerzas Militares y sus familias.

- Riesgo para la Seguridad de la Información: La falta de un plan de continuidad del negocio puede aumentar el riesgo de pérdida o compromiso de datos sensibles de salud en caso de una interrupción operativa. Sin protocolos establecidos para la gestión de datos durante emergencias, la DIGSA corre el riesgo de enfrentar violaciones de seguridad de la información que podrían tener graves repercusiones legales y reputacionales.

- Impacto en la Eficiencia Operativa: La falta de mecanismos de continuidad del negocio puede generar confusión y caos en la DIGSA durante situaciones de crisis, lo que afecta la eficiencia operativa y la capacidad de respuesta del personal. Sin pautas claras y procedimientos establecidos, es probable que se produzcan retrasos en la toma de decisiones y en la ejecución de acciones correctivas, lo que podría agravar aún más la situación.

- Desafíos en la Recuperación Post-Evento: En ausencia de un plan de continuidad del negocio, la DIGSA enfrentaría desafíos significativos en la etapa de recuperación después de un evento

disruptivo. La falta de lineamientos claros para la restauración de sistemas y procesos podría prolongar el tiempo de inactividad y dificultar la vuelta a la normalidad de las operaciones, lo que tendría un impacto negativo en la prestación de servicios de salud.

11. Portafolio de Iniciativas, Proyectos y Mapas de ruta

11.1. Proyectos

La Dirección General de Sanidad Militar (DIGSA) de Colombia enfrenta constantes desafíos en su misión de brindar servicios asociados a la atención médica y de sanidad de calidad a las Fuerzas Militares (Ejército, Armada y Fuerza Aeroespacial) y sus familias. En un entorno en constante evolución, donde la tecnología juega un papel fundamental en la mejora de los servicios de salud, surge la necesidad imperante de formular un proyecto de inversión en tecnología que permita modernizar y optimizar los procesos dentro de la institución

Este proyecto tiene como objetivo principal aprovechar las innovaciones tecnológicas para fortalecer la infraestructura informática y de comunicaciones de la Dirección General de Sanidad Militar, facilitando así la prestación eficiente de servicios médicos, la gestión de recursos y la toma de decisiones fundamentadas en datos. A través de la implementación de soluciones tecnológicas avanzadas, se busca incrementar la calidad, la accesibilidad y la efectividad de la atención médica, garantizando al mismo tiempo la seguridad y la confidencialidad de la información en salud.

En este contexto, la formulación de este proyecto de inversión representa un paso crucial hacia la modernización y la mejora continua de la infraestructura de salud militar en Colombia. Por tanto, es fundamental realizar un análisis detallado de las necesidades y los desafíos específicos que enfrenta la institución, así como identificar las tecnologías más adecuadas y los recursos necesarios para su implementación exitosa. Este proyecto no solo contribuirá al fortalecimiento de la capacidad operativa de la Dirección General de Sanidad Militar, sino que también tendrá un impacto significativo en el bienestar y la salud de quienes sirven a la patria.

El Grupo de Sistemas Integral de Información – Tecnologías de la Información y las Comunicaciones aplicando la metodología de marco lógico realizo la construcción del árbol de problemas de acuerdo a lo hallazgos y brechas identificados en el capítulo anterior, a continuación, se presenta la cadena de valor del proyecto "*Fortalecimiento del Modelo de Gestión de las Tic para ofrecer más y mejores servicios tecnológicos en procura del mejoramiento de la calidad de vida de los grupos sociales objetivo de la DIGSA"*.

1. El objetivo específico 1 de "*Proveer Un Sistema De Información Integrado*" se centra en la implementación de un sistema integral que permita la gestión eficiente y unificada de la información en toda la institución. Este objetivo busca superar la fragmentación y la falta de cohesión entre los sistemas de información existentes, facilitando así la toma de decisiones informadas y la mejora de los procesos operativos y administrativos.

2. El objetivo específico 2 "*Propender por la Actualización de los Servicios Tecnológicos de DIGSA*" dentro del proyecto de inversión de modernización tecnológica de la Dirección General de Sanidad Militar (DIGSA) se enfoca en garantizar que los servicios tecnológicos proporcionados por la Entidad estén alineados con los últimos avances y mejores prácticas en el campo de la tecnología de la información y la comunicación. Este objetivo busca mejorar la infraestructura tecnológica de la DIGSA y optimizar la entrega de servicios digitales a los usuarios internos y externos.

3. El objetivo específico 3 "*Fortalecer el Conocimiento Tecnológico de los Servidores Públicos de la DIGSA*" se enmarca en el proyecto de inversión de modernización tecnológica de la Dirección General de Sanidad Militar (DIGSA). Se centra en el fortalecimiento de las capacidades y competencias tecnológicas del personal que labora en DIGSA, con el fin de optimizar el uso y aprovechamiento de las

nuevas tecnologías implementadas y garantizar una transición exitosa hacia un entorno tecnológico más avanzado.

4. El objetivo específico 4 "*Implementar el Sistema de Gestión de Continuidad de Negocio"* se enmarca en el proyecto de inversión de modernización tecnológica de la Dirección General de Sanidad Militar (DIGSA) y se centra en la implementación de un Sistema de Gestión de Continuidad de Negocio (SGCN) que garantice la capacidad de DIGSA para mantener sus operaciones críticas en caso de interrupciones o eventos adversos.

11.1.1. Cadena de Valor Año 1

Tabla 41. Cadena de Valor Año 1

Año 1					
Objetivos Específicos	Fines o Propósitos Directos	Fines o Propósitos Indirectos	Acciones Clave	Proyecto	Valor Estimado
1. Proveer un Sistema de Información Integrado	Proveer Información A Los Niveles Operativos, Tácticos Y Estratégicos Que Contribuyan A La Efectiva Toma De Decisiones	Mejorar la Calidad de la Información	Mejora de Procesos de Captura de Datos	Actualización de los Sistemas de Información Asistencial de la Entidad	$ 1.000.000.000
				Implementación del Sistema Integrado de Gestión Documental	$ 2.500.000.000
				Implementación de Pertinencia en el Proceso de Prescripción de Medicamentos	$ 500.000.000
				Actualización del Portal Web Y Ampliar Portafolio de Servicios en Internet Ofrecidos por la DIGSA (Incluye Portal de Servicios, Chatbot y APP Móvil	$ 800.000.000
			Estandarización de Datos	Sistema de Inteligencia de Negocios, Gobierno y del Dato Y Analítica de Datos para la Prestación de los Servicios en Salud	$ 1.500.000.000
			Validación y Verificación de Datos		
			Garantía de Calidad de Datos		
			Capacitación del Personal		
Total, Objetivo 1					**$6.300.000.000**
2. Propender Por La Actualización	Mejorar la Prestación de los	Satisfacción en el Uso de los	Identificación de Necesidades y Expectativas	Campaña de Actualización y Caracterización de	$ 600.000.000

Año 1					
Objetivos Específicos	Fines o Propósitos Directos	Fines o Propósitos Indirectos	Acciones Clave	Proyecto	Valor Estimado
De Los Servicios Tecnológicos De DIGSA	Servicios Tecnológicos de la DIGSA	Servicios Tecnológicos por Parte de los Grupos Sociales Objetivo	Diseño Centrado en el Usuario	Afiliados De DIGSA	
			Medición de la Satisfacción del Usuario		
			Gestión de Expectativas		
			Capacitación y Soporte		
			Personalización de Servicios		
	Ampliar la Cobertura de Servicios Tecnológicos de DIGSA	Transmitir la Oferta de Valor de DIGSA a los Grupos Sociales Objetivo	Desarrollo de Estrategias de Comunicación	Sistemas de Apoyo para la Autoatención de los Afiliados de la DIGSA	$ 800.000.000
			Identificación de Mensajes Clave		
			Segmentación de Audiencias		
			Creación de Materiales de Comunicación		
			Capacitación del Personal		
			Evaluación de Impacto		
Total, Objetivo 2					**$1.400.000.000**
3. Fortalecer El Conocimiento Tecnológico De Los Servidores Públicos De La DIGSA	Mejorar el Uso Y Apropiación de los Servicios Tecnológicos de La DIGSA	Adecuado Uso Y Apropiación de las Tic por Parte de los Servidores Públicos de DIGSA, Disminuyendo la Dependencia de Terceros	Capacitación Especializada en TIC	Servicios de Fortalecimiento del Conocimiento de Tecnologías de la información y Las Comunicaciones a Servidores Públicos de la DIGSA	$ 20.000.000
			Promoción de la Autonomía Tecnológica		
			Desarrollo de Capacidades Internas		
			Establecimiento de Procedimientos Internos		
			Facilitación de Recursos y Herramientas		
			Monitoreo y Evaluación Continua		
Total, Objetivo 3					**$20.000.000**
4.Implementar el Sistema de Gestión de	Operativizar El Sistema De Gestión De	Operación Del Negocio 7X24	Establecimiento de Procesos de Monitoreo Continuo	Implementar Las Buenas Prácticas De La Norma Técnica 27001	$ 400.000.000

Año 1					
Objetivos Específicos	Fines o Propósitos Directos	Fines o Propósitos Indirectos	Acciones Clave	Proyecto	Valor Estimado
Continuidad de Negocio	Continuidad De Negocio De La DIGSA			(Seguridad De La Información)	
				Desarrollo de un Análisis de Impacto del Negocio – BIA (Business Impact Analysis)	$ 400.000.000
Total, Objetivo 4					**$800.000.000**
Total, Año 1					**$8.520.000.000**

Fuente: Elaboración propia SISAM

11.2. Hoja de Ruta PETI 2023-2026

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	0,00	0,00	0,00	0,00	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	0,00	0,00	0,00	0,00	Soporte remisión

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**	
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 al Comité Institucional de Gestión y Desempeño	Anual	0,00	0,00	0,00	0,00	Acta aprobación
Implementación del modelo de Gestión y Gobierno de TI - MGGTI		Establecer un modelo para la gestión y gobierno de TI para el SSFM.	Trimestral	0,00	0,00	0,00	0,00	Informes trimestrales vigencia 2027
Implementación del Plan de Transformación Digital al Interior del SSMF.	Implementación del Plan de Transformación Digital al Interior del SSMF.	Implementación y monitoreo de la hoja de ruta del documento Modelo de Gobierno de Datos	Trimestral	0,00	0,00	0,00	0,00	Informes trimestrales vigencia 2025
Seguridad de la información	Realizar un análisis periódico de los controles implementados en cada uno de los riesgos.	Informe trimestral de los riesgos que se han mitigados a través de medidas de seguridad.	Trimestral	0,00	0,00	0,00	0,00	Informes trimestrales vigencia 2025
Seguridad de la información	Copia de Seguridad y Recuperación de Datos.	Implementar una estrategia de respaldo de datos y planes de recuperación ante desastres.	Trimestral	0,00	0,00	0,00	0,00	Informes trimestrales vigencia 2025
Seguridad de la información	Protección contra Malware y Amenazas Externas.	Implementar soluciones de protección contra malware y antivirus.	Trimestral	0,00	0,00	0,00	0,00	Informes trimestrales vigencia 2025
Seguridad de la informacion	Proceso de gestión y parcheo de vulnerabilidades de sistemas.	Por medio de una aplicación de monitoreo detectar lo que este desactualizado y corregir las	Trimestral	0,00	0,00	0,00	0,00	Informes trimestrales vigencia 2025

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**	
		novedades encontradas.						
Implementación y monitoreo de la hoja de ruta del documento Modelo de Gobierno de Datos	Implementación Modelo Gobierno de Datos	Implementación y monitoreo de la hoja de ruta del documento Modelo de Gobierno de Datos	Trimestral	0,00	0,00	0,00	0,00	Informes trimestrales vigencia 2026
Capacitación Modelo de Gestión y Gobierno de TI - MGGTI - Marco de Referencia de Arquitectura Empresarial	Estrategia de Capacitación en Gobierno de Datos	Capacitación dirigida a Subdirectores, Coordinadores, Lideres de Áreas del Staff, Gestores de Calidad de la DIGSA.	Semestral	0,00	0,00	0,00	0,00	Informe Trimestral Capacitaciones
Capacitación Dominio Gestión de la Información (Modelo de Gestión y Gobierno de TI - MGGTI - Marco de Referencia de Arquitectura Empresarial)		Capacitación dirigida a Subdirectores, Coordinadores, Lideres de Áreas del Staff, Gestores de Calidad de la DIGSA.	Semestral	0,00	0,00	0,00	0,00	Informe Trimestral Capacitaciones
Capacitación Modelo de Gobierno de Datos DIGSA		Capacitación dirigida a Subdirectores, Coordinadores, Lideres de Áreas del Staff, Gestores de Calidad de la DIGSA.	Trimestral	0,00	0,00	0,00	0,00	Informe Trimestral Capacitaciones
Capacitación Gestión de la Información		Capacitación dirigida a Subdirectores, Coordinadores, Lideres de Áreas del Staff, Gestores de Calidad de la DIGSA.	Semestral	0,00	0,00	0,00	0,00	Informe Trimestral Capacitaciones

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**	
Capacitación Gestión del Cambio para el Gobierno de Datos en la DIGSA		Capacitación dirigida a Subdirectores, Coordinadores, Lideres de Áreas del Staff, Gestores de Calidad, Funcionarios de la DIGSA	Trimestral	0,00	0,00	0,00	0,00	Informe Trimestral Capacitaciones
Capacitación Gestión del Ciclo de Vida de la Información		Capacitación dirigida a Subdirectores, Coordinadores, Lideres de Áreas del Staff, Gestores de Calidad de la DIGSA.	Semestral	0,00	0,00	0,00	0,00	Informe Trimestral Capacitaciones
Capacitación para la implementación del Catálogo de Materiales e Insumos Médicos DIGSA versión 1 y el uso de este		Capacitación dirigida al Personal logístico de sanidad	Trimestral	0,00	0,00	0,00	0,00	Informe Trimestral Capacitaciones
Capacitación para el manejo de la funcionalidad en Microsoft office 365 - Power Apps rol Coordinador Flujo de Información DIGSA		Capacitación dirigida a Coordinadores, Lideres de Áreas del Staff, Gestores de Calidad de la DIGSA.	Semestral	0,00	0,00	0,00	0,00	Informe Trimestral Capacitaciones
Capacitaciones de reinducción, actualización, manejo y roles Power Apps Flujo de Información - Calendarización 2025.		Capacitación dirigida a Coordinadores, Lideres de Áreas del Staff, Gestores de Calidad de la DIGSA.	Semestral	0,00	0,00	0,00	0,00	Informe Trimestral Capacitaciones
Capacitación para Gestión del Ciclo de		Capacitación dirigida a Coordinadores, Lideres de	Semestral	0,00	0,00	0,00	0,00	Informe Trimestral Capacitaciones

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**	
Vida de los Datos		Áreas del Staff, Gestores de Calidad de la DIGSA.						
Plan de Cultura y Apropiación TD.	Programa de Transformación Digital DIGSA 2025	Definir y desarrollar un plan de cultura y apropiación con un componente de alfabetización digital y gestión de conocimiento, otro de medición de la apropiación de la transformación digital de la DIGSA.	Anual	0,00	0,00	0,00	0,00	Documento Plan
Nivel de Avance Dominios Modelo de Gestión y Gobierno de TI		Iniciar la implementación Modelo de Gestión y Gobierno de TI Proyectado acorde al Marco de Arquitectura Empresarial	Anual	0,00	0,00	0,00	0,00	Informe trimestral
Modelo de Gobernanza de Datos DIGSA		Establecer de la gobernanza de los datos producidos para soportar los datos abiertos, la interoperabilidad y la analítica institucional de la DIGSA	Anual	0,00	0,00	0,00	0,00	Informe trimestral
Modelo de Seguridad y Privacidad de la Información.		Mantener los instrumentos y controles de seguridad y privacidad de la información existentes y proponer e implementar los conforme al MSPI con un enfoque de	Anual	0,00	0,00	0,00	0,00	Informe trimestral

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**	
		ciberseguridad para el entorno digital de la salud pública.						
Digitalización y automatización de trámites y OPAs		Identificar los trámites y OPAs del servicio de Salud que podrían ser digitalizados o automatizados, priorizar y realizar su proceso de registro en el SUIT y definir los requisitos para su transformación digital.	Anual	0,00	0,00	0,00	0,00	Informe trimestral
Automatización de procesos internos de la DIGSA		Identificar, analizar, diseñar e implementar soluciones ágiles de automatización de procesos internos para la prestación de los servicios de salud, con el fin de facilitar la optimización de los procesos con el uso de las tecnologías de la información.	Anual	0,00	0,00	0,00	0,00	Informe trimestral
Datos para la toma de decisiones informadas		Consolidar una estrategia consciente de analítica institucional que gestione el aprovechamiento de los datos para la toma de decisiones tácticas y operativas en Salud.	Anual	0,00	0,00	0,00	0,00	Informe trimestral

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**	
Datos abiertos DIGSA para el sector salud		Consolidar y acondicionar la publicación de datos abiertos DIGSA y postular la implementación al sello de excelencia de MinTIC para Gobierno abierto.	Anual	0,00	0,00	0,00	0,00	Informe trimestral
Adopción y uso de tecnologías emergentes en Salud		Identificar en la DIGSA casos de uso para el uso de tecnologías emergentes o de 4RI, definir los requisitos, desarrollar e implementar un piloto con la(s) tecnología(s) escogida(s).	Anual	0,00	0,00	0,00	0,00	Informe trimestral
Servicios DIGSA de ciudades y territorios inteligentes en Salud		Identificar servicios digitales DIGSA que apliquen para ciudades y territorios inteligentes en Salud, para certificar ante el MinTIC aquellos más maduros, luego realizar su promoción y posicionamiento.	Anual	0,00	0,00	0,00	0,00	Informe trimestral
Transformación de SALUD.SIS		Iniciar con la implementación de Transformación del Sistema de Información SALUD.SIS de la DIGSA para mejorar su funcionalidad, hacerlo interoperable, abierto y sostenible,	Anual	0,00	0,00	0,00	0,00	Informe trimestral

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**	
		cumpliendo los criterios de usabilidad, accesibilidad, .						
Servicios de Información Actualizados	Desarrollar módulos de la Vertical de Salud	Servicio de fábrica de software, encaminado a efectuar desarrollar ajustes a cambios normativos y módulos de cirugía, hospitalización, enfermería y urgencias.	Anual	0,00	0,00	316.507.273,13	0,00	Informe trimestral
		Actualización capa de aplicación y arquitectura de datos	Anual	0,00	0,00	500.000.000,00	0,00	Informe trimestral
		Continuación desarrollo e implementación ecosistema de interoperabilidad con red prestadora de servicios de salud	Anual	0,00	0,00	500.000.000,00	0,00	Informe trimestral
Mantenimiento servicios Tecnológicos	Gestionar la adquisición del servicio de Data Center para el desarrollo e implementación del Sistema de Información a nivel nacional	Servicio de DATACENTER MDN (Productivo y continuidad de negocio)	Anual	0,00	0,00	1.302.545.085,88	0,00	Informe trimestral
	Realizar soporte técnico (Mantenimiento de software, mesa de servicio)	Contratación servicio de soporte y mantenimiento de software	Anual	0,00	0,00	1.300.000.000,00	0,00	Informe trimestral
		Contratación soporte y mantenimiento plataforma	Anual	0,00	0,00	400.000.000,00	0,00	Informe trimestral

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**	
		PACS integrada (DIGSA - FAC)						
	Actividades para mantenimiento por Gastos de Funcionamiento	Computadores de escritorio	Anual	0,00	0,00	50.000.000,00	0,00	Informe trimestral
		Licenciamiento conmutador telefónico	Anual	0,00	0,00	18.500.000,00	0,00	
		Licenciamiento soporte firewall	Anual	0,00	0,00	321.000.000,00	0,00	
		Licenciamiento end point seguridad	Anual	0,00	0,00	168.525.000,00	0,00	
		Solución en seguridad de correo electrónico.	Anual	0,00	0,00	85.600.000,00	0,00	
		Servicio SOC, NOC, SOAR, SASE	Anual	0,00	0,00	600.000.000,00	0,00	
		(Certificado SSL) 81112103	Anual	0,00	0,00	3.500.000,00	0,00	
		Canales dedicados y conexión a internet fortaleza	Anual	0,00	0,00	166.920.000,00	0,00	
		Continuidad del negocio - servicio en la nube (Adquirir Créditos de AZURE)	Anual	0,00	0,00	30.000.000,00	0,00	
		Licenciamiento soporte y mantenimiento - KACTUS	Anual	0,00	0,00	75.000.000,00	0,00	
		Licenciamiento de suite adobe Acrobat pro - licencia adobe stock	Anual	0,00	0,00	9.630.000,00	0,00	
		Sistema de nómina Paoyer	Anual	0,00	0,00	200.000.000,00	0,00	
		Licencias SAP DIGDA	Anual	0,00	0,00	100.000.000,00	0,00	
		Licenciamiento Office 365 para servicios en la nube por un año+Devops	Anual	0,00	0,00	486.400.000,00	0,00	
		Licenciamiento sistema	Anual	0,00	0,00	336.000.000,00	0,00	

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**	
		operativo Datacenter						
		Licenciamiento Win server CAL License& software Assurance Open	Anual	0,00	0,00	50.000.000,00	0,00	
		Extensión garantías de servidores	Anual	0,00	0,00	68.480.000,00	0,00	
		Página web - hosting	Anual	0,00	0,00	165.000.000,00	0,00	
		Extensión de garantía NAS Pro Support Plus	Anual	0,00	0,00	440.000.000,00	0,00	
		Soporte ODA (Oracle Premier Support for System) – Debe Incluir Cambio de Partes en Sitio	Anual	0,00	0,00	60.000.000,00	0,00	
		Renovación Soporte OnBase	Anual	0,00	0,00	420.000.000,00	0,00	
		Renovación licencias Jaspersoft	Anual	0,00	0,00	659.600.000,00	0,00	
		Renovación licencias NGINEX	Anual	0,00	0,00	52.000.000,00	0,00	
		Renovación licencias ZENDESK	Anual	0,00	0,00	87.200.000,00	0,00	
		Mensajería de SMS y EMAILS	Anual	0,00	0,00	70.000.000,00	0,00	
		Licencia Visor interoperabilidad	Anual	0,00	0,00	100.000.000,00	0,00	
		Digiturno	Anual	0,00	0,00	11.000.000,00	0,00	
		Adquisición de UPS Datacenter DIGSA	Anual	0,00	0,00	78.500.000,00	0,00	
		Sede Electrónica	Anual	0,00	0,00	500.000.000,00	0,00	

Fuente: Elaboración propia GRUGI-SISAM

12. BIBLIOGRAFÍA

- 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 2023 – 2026
- Guía para la formulación y seguimiento de los planes institucionales del SSFM-DIGSA, Septiembre del 2024
- Documento - versión actualizada del modelo de gestión TI 2023v2.0
- DESEMPEÑO INSTITUCIONAL. Manual Operativo del Modelo integrado de Planeación y Gestión. Edu.co Recuperado el 4 de septiembre 2024, de https:/www.sena.edu.co/esco/sena/Documents/Manual%Operativo%20MIPG%20v5.pdf
- Directiva Permanente No. 012007744702 /MDN-COGFM-JEMCO-DIGSA-SUBSA- GROSD-AREIN - 13 del 05 de Julio del 2024. [Dirección General de Sanidad Militar]"Lineamientos para la tipificación de los establecimientos de sanidad militar del Subsistema de Salud de la Fuerzas Militares y funciones del componente de Salud Operacional

ANEXO 1

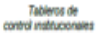
Tendencias tecnológicas construcción PETI 2024					
TIPO	PROC	AREA	NOMBRE	DESCRIBA LA TECNOLOGÍA REQUERIDA	NECESIDAD TECNOLOGIAS 4RI
MISIONAL	PROASS	GROSD	**Cloud Computing**	Se requiere BI en cada uno del os equipos del Grupo GROSD	
			Inteligencia Artificial - Machine Learning	Se requiere crear un modelo en IA que ayude a la predicción de la entrega de medicamentos asociada a cada una de las patologías que presentan los usuarios del SSFM y establecer la demanda.	
			Big Data	Requerimos espacio en un servidor para alojar los altos volumentes de mediamentos y todo lo respectivo a CTC y Tutelas	
			Informacion espacial Georreferenciador - mapas	Requerimos un Mapa automatizado conde esten los ESM con su respectivo portafolio, población adscrita, perfil epidemiológico.	
			Analítica	Se requiere BI en cada uno del os equipos del Grupo GROSD	
			Plataformas de Ciberseguridad	Lo suministrado en general para la entidad y el sector defensa	
			Plataforma colaborativa	Creación de Share Point	
			Inteligencia Artificial adaptativa o de entrenamiento	Crear una aplicación mediante IA para todo el tema de autorizaciones y agendamiento de citas	
MISIONAL	PROSOPE	GRUSO	**Cloud Computing**	Microsoft Azure: Ofrece servicios de computación, almacenamiento y bases de datos, entre otros.	
				Google Cloud Platform (GCP): Incluye servicios de infraestructura y herramientas para desarrollo y análisis de datos.	
				Google Workspace: Conjunto de herramientas de productividad, como Gmail, Docs y Drive.	
				Heroku: Permite a los desarrolladores construir, ejecutar y operar aplicaciones completamente en la nube.	
			Inteligencia Artificial - Machine Learning	Scikit-learn: Biblioteca en Python que proporciona herramientas simples y eficientes para el análisis de datos y machine learning.	
				Pandas: Biblioteca de Python para la manipulación y análisis de datos, especialmente útil para la limpieza y preparación de datos.	
				Apache Spark: Framework para el procesamiento de grandes volúmenes de datos, que incluye capacidades de machine learning a través de MLlib.	
			Internet de las Cosas	Grafana: Herramienta de visualización de datos que se puede utilizar para crear paneles y gráficos en tiempo real a partir de datos IoT.	
				Tableau: Herramienta de visualización de datos que puede integrarse con fuentes de datos IoT para análisis avanzados.	
			Big Data	Apache Hadoop: Framework que permite el almacenamiento y procesamiento de grandes volúmenes de datos en clústeres distribuidos. Incluye el sistema de archivos HDFS y el motor de procesamiento MapReduce.	
				Apache Spark: Motor de procesamiento de datos en tiempo real que ofrece una interfaz más rápida y fácil de usar que Hadoop, ideal para análisis en tiempo real y aprendizaje automático.	
				Apache NiFi: Herramienta para automatizar el flujo de datos entre sistemas, facilitando la integración de datos en tiempo real.	
				Talend: Plataforma de integración de datos que proporciona herramientas para ETL y calidad de datos.	
			Informacion espacial Georreferenciador - mapas	ArcGIS: Una de las plataformas SIG más populares, ofrece herramientas avanzadas para el análisis espacial, visualización y gestión de datos geográficos.	
				MapInfo: Plataforma SIG que se utiliza para crear mapas, realizar análisis espaciales y gestionar datos geográficos.	
				Mapbox: Plataforma que ofrece mapas personalizados y herramientas para desarrolladores, con capacidades avanzadas de visualización y diseño.	
			Analítica	Microsoft Power BI: Plataforma de análisis de datos que facilita la creación de informes y dashboards a partir de múltiples fuentes de datos, con integración profunda en el ecosistema de Microsoft.	
				R: Lenguaje de programación y entorno de software para análisis estadístico y visualización de datos. Tiene una amplia gama de paquetes para diferentes tipos de análisis.	
				SAS: Plataforma de análisis avanzada que incluye herramientas para análisis predictivo,	

TIPO	PROCESO	AREA	NOMBRE	DESCRIBA LA TECNOLOGÍA REQUERIDA	
MISIONAL	PROGERI	GRERI	**Cloud Computing**	Solicitamos Herramientas para planificación de proyectos , Solicito acceso a licencia Power BI Desktop ó Nube para transformar y modelar datos para los profesionales en analitica de datos., visualizacion avanzada cpn Tableau	
			Inteligencia Artificial - Machine Learning	KNIME: PRUEBA PILOTO PARA MODELOS PREDICTIVOS A MEDIANO Y LARGO PLAZO DE MORBILIDAD	
			Big Data	Motor bases de datos robustas con enfasis en software en inteligencia de negocios	
			Informacion espacial Georreferenciador - mapas	solicitud de sofware (mapinfo - aqregis) para geoubicación de clientes en mapas de IGAC gratuitos desde datos abiertos. El analisis especializado con uso en linea de Epi-info entre otros, capacitaciones	
			Analítica	Requerimos Adquisicion de licencias Python, R, Knime entre otros software en analitica de datos. Visualizacion y manejo analitico bajo herramientas de inteligencia de negocios	
			Plataforma colaborativa	revisar que plataforma colaborativa y de manera segura, permite interaccion de datos compartidos con DISAN y JEFSA	
			Inteligencia Artificial adaptativa o de entrenamiento	Requerimos una herramienta con (RPA) Automatización de procesos repetitivos bajo el uso de IA o robotica, para aumentar productividad y minimizar error humano Microsoft 365 One Drive: Es valioso poder contar con servidores de almacenamiento de datos y aplicaciones, a través de Internet.los cuales permiten acceso de manera remota a la informacion que se requiere en caso de estar fuera de la DIGSA, para poder accader a iformacion y hacer analisis de grandes volumenes de Datos, quedando guardados en la nube con copia de seguridad	
				Migración de datos y bases de datos de la pagina del Ministerio de Salud y Proteccion Social relacionados con CUPS, CUMS, DCI, productos de nutrición componentes de las mezclas unidades de compensación, MIPRES, entre otros.	
				Alertas de proyectos normativos y de emision de politicas en los territorios y pais para toma de decisiones y ajustes necesarios desde la planeación en salud hasta la prestacion de servicios y provision de tecnologias en salud.	
				Acceso a recursos electronicos google scholar, micorosoft academic search, dialnet, redalyc, scielo, redib, Eric, Ref seek, springer link, web of science, bio one complete, willey Online, science Direct, oxford academy, pubmed, scopus, cambridge care entre otros	
			Cloud Computing	Microsoft 365. Microsoft Azure. Incluyen almacenamiento, procesamiento, redes, bases de datos, inteligencia artificial, análisis de datos y más.	
				Un sistema de acceso amplio que permita de manera sencilla y segura que el Funcionario del Sistema de Calidad en Salud de la DIGSA Cargue, Descargue y Visualice el material de apoyo requerido para el fortalecimiento de los conocimientos y asi como de la actualizacion documental del SSFM.	
				Se solicita la adquisisición de ALMERA O El BALANCED SCORECARD, herramientas que integran la estrategia de la organización con la operación diaria, facilitan la implementación, evaluación y mantenimiento de sistemas de calidad alineándolos con los sistemas de control interno, administración de riesgos y sistemas para evaluar la gestión de la organización.	
				Se recomienda la adquisicion de Azure de Microsoft para la intergracion de productos relacionados, servicios y aplicaciones externas requeridas para trabajos hibridos y una conexion mas segura en la nube, este aporte podria impactar en la innovacion para análisis de datos y aplicacion del Internet de las cosas.	
				Es importante poder utilizar las bondades de Inteligencia Artificial para mejorar los Diagnosticos médicos, sobre todo con proyeccion de imagenes Diagnosticas para lograr analisis de imagenes con Dx mas certeros , en procesos Quirurgicos es adecuado para la presicion del procedimiento y que estos sean poco invasivos. para la investigacion y creacion de tecnologías en salud , todo contrubuye a tener mejores resultados clínicos y eficiencia de los recursos	
				Un algoritmo que transforma la descripción en el código correspondiente de CUPS, CUM u otros, en su descripcion o viceversa. Esto permite que los sistemas de salud usen términos	

MISIONAL	PROAS	GRUAS	**Inteligencia Artificial - Machine Learning**	recomendaciones basadas en la probabilidad de que necesitaran atención adicional. Como resultado, el hospital pudo reducir el número de readmisiones innecesarias y ahorrar significativamente en costos de atención médica. CHAT GPT (bases ASIS Y SISMED) Simulaciones y modelado de datos Trascriptor de órdenes de historias clínicas a partir de escucha de consulta	
				El Sistema debe permitir al o los Funcionarios de Garantía de la Calidad en Salud de la DISAN (EJC,ARC) y JEFSA correspondiente, formular en el Módulo de Mejoras del Sistema de Calidad en Salud, las Acciones Correctivas Institucionales, luego del Análisis de los Criterios No Cumplidos por sus ESM en la Autoevaluación de Capacidad Técnico Científica, permitiendo incorporar sistemas integrados que permitan visualizar mediante semaforización las mejoras del Sistema de Calidad en Salud, cuyo apoyo con el machine learnig permita identificar los comportamientos en los datos aportando mayor eficacia y disminicion de los tiempos al momento de la verificacion de los datos suministrados por los ESM a DISAN(EJC,ARC) a JEFSA	
				Se requiere la actualizacion y capacitacion de la implementacion de herramientas actuales cuyo desarrollo de el alcance para encontrar patrones y correlaciones en grandes data sets, logrando apoyar las decisiones y proyecciones en base a los analisis.	
			Internet de las Cosas	Posibilidad de tener conectividad con herramientas como SMARTWATCH,Monitoreo de glucosa,Monitorización de la frecuencia cardíaca y de mas que tengan los pacientes afiliados al SSFM para capturar informacion de forma real en historia clinica.	
				Implementar plataformas de conocimiento colaborativas donde la información recopilada por IoT se actualice en tiempo real y esté disponible para todos los equipos involucrados desde el aseguramiento hasta la prestación en normatividad, CUPS,temas de interes, etc	
				Migración de datos y bases de datos de la pagina del Ministerio de Salud y Proteccion Social relacionados con CUPS, CUMS, DCI, productos de nutrición componentes de las mezclas unidades de compensación, MIPRES, entre otros.	
				Alertas de proyectos normativos y de emision de politicas en los territorios y pais para toma de decisiones y ajustes necesarios desde la planeación en salud hasta la prestacion de servicios y provision de tecnologias en salud.	
				Dispositivos biométricos portátiles para supervisar la salud de los pacientes de forma remota, Los servicios biométricos y de telemedicina forman un dúo dinámico que trabaja mano a mano para mejorar la atención a los pacientes. Con los dispositivos portátiles y los sensores biométricos, los proveedores de atención médica pueden monitorear la salud de los pacientes de forma remota, lo que permite tomar decisiones informadas y brindar una atención personalizada	
				Se proyecta la posibilid de incorporar elementos IoT para generar conexiones y fortlacer la informacion en tiempo real desde cualquier dispositivos externo, logrando mejorar los resultados e identificacion de manera mas eficientes las problematicas presentadas.	
			Big Data	Es relevante contar con sistemas de captura de grandes volumenes de informacion que puedan ser procesados a altas velocidades pudiendo obtener como resultado estructuras de informacion que permitan ser analisados para la toma de decisiones en la DIGSA, realizar estudios de impactos en salud, suficiencia de recursos.	
				Repositorio de los historicos en lineamientos, proyectos de investigación en salud y normativa aplicada al subsistema	
				Herramientas de Modelación poblacional con análisis de datos en tiempo real. Acceso a Software de Modelos Financieros y Proyecciones Health Catalyst o Tableau: Herramientas de visualización y análisis financiero que permiten construir modelos prospectivos sobre costos de enfermedades, evaluar desviaciones presupuestales y realizar simulaciones financieras serían esenciales para mejorar la sostenibilidad del sistema.	
				Desarrollar una funcionalidad en el módulo (Business Intelligence) en la cual se pueda capturar la información de todos los indicadores propuestos para el SSFM, entre los cuales se incluyan los del Sistema de Calidad en Salud. El sistema debe permitir al funcionario del Sistema de Calidad en Salud de la DIGSA, DISAN (EJC, ARC) y JEFSA consultar los ESM registrados en el Módulo de Portafolio de Servicios y capacidad instalada, adicional las herramientas para que el Funcionario de Garantía de la Calidad en Salud del ESM cargue como archivo adjunto en Formato PDF los documentos de soporte de las novedades registradas, que se contemplan en la Normatividad propia del SSFM o las que la modifiquen o sustituyan, de tal manera que la	

TIPO	PROCESO	AREA	NOMBRE	DESCRIBA LA TECNOLOGÍA REQUERIDA	
ESTRATEGICO	PROCEGC	ARCOM	**Cloud Computing**	solicitamos Herramientas con más capacidad en la nube, ya que el contenido que se maneja m	
				Se solicitan herramientas de diseño y de optimización del diseño gráfiuco para imagen faja y video. Acceso a bancos de imágenes para poder optimizar el desarrollo de piezas.	
			Inteligencia Artificial - Machine Learning	Monitoreo de publicaciones y aparición en medios y redes sociales.	
			Robótica y drones	cámara profesional actualizada, drones para realizar tomas aéreas, micrófonos de solapa y tripodes.	
				ESTABILIZADOR DE IMAGEN PARA CELULAR PARA REALIZAR EN VIVOS	
			Big Data	Se requieren 2 tarjetas de video y ampliación de la capacidad de la velocidad de 3 de los computadores asignados al área en virtud a la cantidad y calidad de los materiales que se almacenan. De igual forma se requieren discos de soporte para poder generar los backup correspondientes.	
			Aplicaciones inteligentes	Mobile Data Science and Intelligent Apps	
				SUIT DE ADOBE PARA DISEÑO DE PIEZAS GRÀFICAS, BANCO DE IMÁGENES Y VIDEO, APLICACIONES DE INTELIGENCIA ARTIFICIAL PARA DISEÑO, APLICACIONES PARA MEDICIÒN DE REDES SOCIALES Y ENVIO DE CORREOS MASIVOS	
			Otra_	Se requiere optiomización del equipo técnico del área con un kit de luces LED, una panel croma y un kit de micr+ófonos inhalambricos de solapa para entrevistas	
APOYO	PROAPA	GRUAA	**Criptografia asimetrica**	se requiere para aplicar la politica de 0 (CERO) papel y agilizar los procedimientos de inventarios con la implementacion de la firma digital	
APOYO	PROGI	GRUGI	**Cloud Computing**	Solicitamos Herramientas para planificación de proyectos . (Microsoft project). Solicito acceso a licencia Power BI Desktop ó Nube para transformar y modelar datos para los profesionales en analitica de datos Gestión d ela Información.	 
			Internet de las Cosas	Detección, transporte, almacenamiento y análisis de datos.	
			Big Data	Solicitud de motores robustos en manejo de datos SQL, ORACLE, MICROSOFT SQL SERVER, OTROS	
			Analítica	Adquisicion de licencias Python, R, Knime entre otros software en analitica de datos	
APOYO	PROALEG	GRULE	**Inteligencia Artificial - Machine Learning**	La implementación de un asistente virtual/chatbot dentro de la pagina de la entidad, puede transformar significativamente la manera en que el grupo de asuntos legales interactúa con los ciudadanos y maneja sus procesos internos. Que tenga la capacidad de responder preguntas comunes sobre procedimientos legales, como historias clínicas y junta medica de manera automática.	
			BlockChain	Implementar una tecnología de blockchain, para verificar la trazabilidad documental de los proceso del grupo por parte de los usuarios el SSFM.	
			Otra_	La implementación de una tecnología que mejore el proceso de recepción / radicación del correo de notificaciones judiciales del grupo es fundamental para trabajar en términos con los despachos judiciales. Además de hacer uso de una política mas ecológica como es la reducción de la cantidad de impresiones realizadas.	
			Otra_	Una actualización del aplicativo de SGDEA, que mejore varios aspectos para tener un uso mas practico y veloz respecto a las actividades diarias, como lo son la generación de radicados, mas estabilidad en el funcionamiento y otras funciones que mejoren los procesos, no solo del Grupo de Asuntos Legales, si no de toda la entidad para tener una comunicación mas fluida.	

TIPO	PROCESO	AREA	NOMBRE	DESCRIBA LA TECNOLOGÍA REQUERIDA	
ESTRATEGICO	PROPLAES	GRUPL	**Cloud Computing**	Solicito acceso a licencia Power BI Desktop y Nube para transformar y modelar datos con destino a los grupos de interés.	
			Analítica	Adquisicion de licencias R para el análisis de datos del Área de Costos y Estadística. Adquisicion de licencia Python para el análisis de datos del Área de Costos y Estadística.	
			Otra...	Se requiere una herramienta tecnológica que permita gestionar los componentes y procesos del SIG, ya mencionados. Esta herramienta puede ser DARUMA, SUITE VISION EMPRESARIAL, ISO TOOLS, ISOLUCIÓN.	
APOYO	PROTH	GRUTH	**Inteligencia Artificial - Machine Learning**	Modelos para el control y gestión de las tendencias en administración de personal que permitan prevenir múltiples situaciones administrativas	
			Internet de las Cosas	Accesos a Visualizadores virtuales de Historias laborales de los funcionarios vinculados como un Escáner de iA para lectura e integración de datos sobre soportes de evidencias	
			Big Data	Un sistema de almacenamiento de datos de información del GRUTH para la administración de personal vinculado en cualquiera de sus estados (Retirados, Activos, con ausentismos y candidatos) SIATH integrado en Datos	
			Informacion espacial Georreferenciador - mapas	Se requiere un paquete de Georreferenciación para clasificación de centros de Trabajo, con el fin de ubicar colaboradores vinculados DIGSA	
			Analítica	Software que permita administración y gestión de Administración de Personal (Presupuesto, Gastos, tipo de contratación y otros)	
			BlockChain	Software que genere reportes transaccionales que permitan el reconocimiento y pago de salarios, prestaciones sociales y demás emolumentos asociados a la vinculación laboral.	
APOYO	PROEFIN	GRUFI	**Plataforma colaborativa**	El Grupo Gestión Financiera solicita VPN, permisos del Ministerio de Defensa Nacional para el aplicativo/Sistema informático SAP.	
APOYO	PROCON	GRUCO	**BlockChain**	Almacenamiento de datos estadisticos para la gestión en el SSFM en procesos contractuales y para almacenamiento de contratos y demas informacion relevante de la cual se pueda tener acceso.	
			Criptografia asimetrica (firma	Implementación de firma digital para procesos juridicos	
			Plataforma colaborativa	Acceso a documentos compartidos entre supervisores y abogados Datos que sean actualizados con SECOP para analisis	

TIPO	PROC	AREA	NOMBRE	DESCRIBA LA TECNOLOGÍA REQUERIDA	
MISIONAL	PROAUPS	GRAPS	**Analítica**	Solicitud de un sistema de información que tenga la opción de realizar análisis estadísticos y generación de gráficas para los resultados de la encuesta de satisfacción de los usuarios.	
			Inteligencia Artificial adaptativa o de entrenamiento	Adaptar un RPA automatizado y con inteligencia artificial para la solicitud de las PQRSR. De igual forma, que la aplicación cuente con análisis estadístico, generación de gráficas, relación de cédulas para identificar varias PQRSR de un mismo usuario (usuarios multiquejosos y/o multiples requerimientos con un mismo asunto), semáforos para seguimiento de las PQRSR (Importancia, número de días hábiles, Indicativo por color), tablero control análisis trámites de PQRSR y alertas.	  Power Automate
			Otra_	Adquisición o desarrollo de un nuevo software que permita mejorar la gestión de la elaboración, desarrollo y análisis de la encuesta de satisfacción de los usuarios o de las diferentes encuestas de la DIGSA.	
APOYO	PROGTIC	SISAM	**Cloud Computing**	1. Se requiere la necesidad de seguir con la adquisicion de estas licencias, para poder asi continuar prestando el servicio a los usuarios de la Direccion General de Sanidad Militar 2 Devops en nube para desarrollos que se realicen en la DIGSA.. 3. maquinas virtuales. Asignar recursos para continuar con la misma plataforma de virtualización	
				Asignar recursos para contratar infraestructura que permita migrar (o tener copias de las aplicaciones que se manejan en la DIGSA Kactus, On Base, entre otros).	
			Inteligencia Artificial adaptativa o de entrenamiento	BPM basado en modelo: este se enfoca en la creación y el uso de modelos visuales para describir y gestionar los procesos. BPM basado en casos: en lugar de seguir flujos predefinidos, se adapta a situaciones específicas o «casos».diseñar, ejecutar, analizar y mejorar continuamente cada proceso de negocio de una organización para orientarlos a objetivos concretos	 Power Automate
				1.Power Automate: Licenciarlo 2. Bots: Automatizar tareas automatizadas (implementar) realizar el levantamiento de informacion de las tareas a automatizar	
			Analítica	Software para análisis de datos predictivo 1.SAP Analytics Cloud.(licenciar) 2. Capacitar SAP Analytics Cloud 3. Power BI: se implemente como habilidades necesarias para el trabajo	 Power Apps
			OTROS	1. Realizar la sincronizacion a dispositivos (Tablet, portatiles, pc) Integrando estas aplicaciones entre como tendencia e innovacion y utilidad de estas herramientas asi: 1. Teams: para uso de sincronizacion de contactos para llamadas. Logrando concetar personal. 1.3 Reconocimiento de aplicaciones de administracion de Office-Gobernanza. 1.2. Interactuar con cada Tablero Digital por Power BI, Power Apps, Forms por Areas de la DIGSA. (estadisticas,analisis de Datos, encuestas entre otras) 2. Eshare: enlaces a dispositivos de interacción multipantalla que hace que la experiencia del usuario facil y dinamica como agradable para entretenimiento en las presentaciones y capacitación de la entidad. Contratar desarrollos de apps relacionadas con el sector salud e integrarlas al sistema de información Salud.sis, como por ejemplo la Telemedicina, es decir, atender consultas médicas a distancia mediante videollamadas, chats o llamadas. Tambien Gestionar citas medicas para que el paciente gestione sus citas	 Tableros de control institucionales  Power BI 
			OTROS	Implementar Plataforma X-ROAD	
			OTROS	Carpeta ciudadana; Integración de Tramites y Sevicios en la Carpeta Ciudadana	
MISIONAL	PROGAFI	GRUGA	**Cloud Computing**	Solicitamos acceso a licencia Power BI Desktop ó Nube para uso y apropiacion en inteligencia de negocios, sharepoint, power automate	 Tableros de control institucionales Power BI 
			Inteligencia Artificial - Machine Learning	Solicitamos software en Predicciones sobre comportamientos, reacciones y tendencias en datos almacenados y clasificados, como python, Knime	
			Big Data	Manejo de altos volúmenes de información y velocidad de los datos por medio de plataformas robustas SQL.	
			Informacion espacial Georreferenciador - mapas	Ubicación espacial de afiliados y/o puntos de atención ESM actulizados mediante tecnologias de geoubicación, mapinfo, arcmap, visualizacion en google maps	  
			Analítica	Manejo de software de inteligencia de negocios para procesos en manipulacion segura de informacion de afiliados	
			Plataforma colaborativa	Inteoperabilidad con informacion de otras plataformas como: SIATH integrado en Datos, registraduria, etc (XROAD)	