DIRECCIÓN GENERAL
DE SANIDAD MILITAR

2026

Gestión Tecnologías de la Información y las Comunicaciones - PROGTIC

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

DIGSA 2026

DIGSA	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	Institucional de Seguridad y Privacidad de la Información PSPI DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-2	
	Vigente	Diciembre 2025	Versión: 4

CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de los cambios
1	Enero 2021	Versión Inicial. Elaboración por primera vez del documento. Este documento corresponde al Procedimiento Coordinación y Suministro de Información DIGSA MDN-COGFM-PROGI-DIGSA-PT.95.1-2 . Este Plan fue aprobado en sesión de Comité de Gestión y Desempeño Institucional, del que hacen parte el Director General de Sanidad Militar, los Subdirectores de Salud, Técnico y de Gestión, y Administrativo y Financiero de la DIGSA, los Directores de Sanidad del Ejército y Armada Nacional, Jefatura de Salud de la Fuerza Aérea y los Coordinadores de Grupo de Planeación Estratégica, Asuntos Legales y Seguimiento y Evaluación de la DIGSA; y documentado mediante Acta N° 0120010254602 de fecha 16 de diciembre de 2020. El documento original está debidamente firmado, reposa en los documentos del proceso asociado y está disponible en, https://www.sanidadfuerzasmilitares.mil.co/, lo anterior en cumplimiento al Decreto 612 de fecha 4 de abril de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”. NOTA PROASIG: 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 está construido de acuerdo con los parámetros de lenguaje claro emitidos por el Departamento Nacional de Planeación.
2	Noviembre 2022	Se actualiza de acuerdo con la información y nueva normativa. Este Plan fue aprobado en sesión de Comité de Gestión y Desempeño Institucional, del que hacen parte el Director General de Sanidad Militar, los Subdirectores de Salud, Técnico y de Gestión, y Administrativo y Financiero de la DIGSA, los Directores de Sanidad del Ejército, Sanidad Naval, Jefatura Salud de la Fuerza Aérea y los Coordinadores de Grupo de Planeación Estratégica, Asuntos Legales y, Seguimiento y Evaluación de la DIGSA; y documentado mediante Acta N° 0122014671502 de fecha 21 de diciembre de 2022. NOTA PROASIG: 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. Fue traducido a lenguaje claro.
3	Diciembre 2024	Se actualiza de acuerdo con la información y nueva normativa. Este Plan fue aprobado en sesión de Comité de Gestión y Desempeño Institucional, del que hacen parte el Director General de Sanidad Militar, los Subdirectores de Salud, Técnico y de Gestión, y Administrativo y Financiero de la DIGSA, los Coordinadores de Grupo de Planeación Estratégica, Asuntos Legales y, Seguimiento y Evaluación de la DIGSA; y documentado mediante Acta N° 0124014880202 /MDN-COGFM-JEMCO-DIGSA-ARDEI-2.25, de fecha 30 de

Versión	Fecha de Aprobación	Descripción de los cambios
		diciembre de 2024. El documento original está debidamente firmado, reposa en los documentos del proceso asociado y está disponible en, https://www.sanidadfuerzasmilitares.mil.co/, lo anterior en cumplimiento al Decreto 612 de fecha 4 de abril de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado NOTA PROASIG: 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	Diciembre 2025	Se actualiza el contexto estratégico interno y externo, tablero de control de indicadores y actividades de acuerdo con los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información 2025 del Ministerio de las Tecnologías de la Información y las Comunicaciones Min Tic. Este Plan fue aprobado en sesión de Comité de Gestión y Desempeño Institucional, del que hacen parte el Director General de Sanidad Militar, los Subdirectores de Salud, Técnico y de Gestión, y Administrativo y Financiero de la DIGSA, los Directores de Sanidad del Ejército, Sanidad Naval, Jefatura Salud de la Fuerza Aérea y los Coordinadores de Grupo de Planeación Estratégica, Asuntos Legales y, Seguimiento y Evaluación de la DIGSA; y documentado mediante Acta N0. 0125013849802 del 11 de diciembre del 2025. NOTA PROASIG: 1. Este documento fue revisado y liberado por PROASIG. 2. La información registrada en el documento es responsabilidad del proceso que lo emite.

DIGSA	PROCESO	Proceso Sistema Integral de la Información - Tecnologías de la Información y las Comunicaciones PROGTIC-Área de Seguridad de la Información AREIN	
	Plan	Institucional de Seguridad y Privacidad de la Información PSPI DIGSA	
	Código	MDN-COGFM-PROGTIC-DIGSA-PL-2	
	Vigente	Diciembre 2025	Versión: 4

CONTROL DE APROBACIÓN

Aprobó:	Comité de Gestión y Desempeño Institucional Acta No. 0125013849802 de 2025	
Revisó:	PD. Julio Cesar Salgado Guerrero Gestión Tecnológicas de la Información y las Comunicaciones PROGTIC Gestor de Calidad	CR. John Jairo Villabon Ramos Subdirector Técnico y de Gestión DIGSA
	TC. Jorge Darwin Guevara Guerrero Coordinador Grupo Sistema Integral de Tecnologías de la Información y Comunicación DIGSA	SP. Miguel Ángel Cardozo Líder Área Seguridad de la Información DIGSA
	SMSM. Edna del Pilar Martínez Páez Grupo Planeación Estratégica DIGSA Área Sistemas Integrados de Gestión PROASIG	
Elaboró:	PD. Roberto Rodríguez Perdomo Grupo Sistema Integral de Información – Tecnologías de La Información y las Comunicaciones DIGSA Área de Seguridad de la Información	

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

1. RESENTACIÓN

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información requiere de la elaboración de una serie de procesos, políticas y procedimientos, de acuerdo a las necesidades, objetivos, requisitos de seguridad, procesos misionales, estructura de la Dirección General de Sanidad Militar DIGSA, y teniendo en cuenta las directrices establecidas para la administración y gestión de riesgos, todo anterior en el marco de lo establecido por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las tecnologías de la información y las comunicaciones, mediante el Decreto Numero.1008 de 2018 “Por el cual se establecen lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo uno del título 9 de la parte dos del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de Información y las Comunicaciones”, Manual de Gobierno Digital y Resolución No. 746 de 2022 “Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021”.

Al interior de la Dirección General de Sanidad Militar DIGSA se desarrollan actividades tendientes a garantizar la integridad, confidencialidad y disponibilidad de los activos de la información, mediante la implementación de un Modelo de Seguridad y Privacidad de la Información, alineado a la norma NTC-ISO-IEC-27001:2013. Este modelo, que se fundamenta en los lineamientos del Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC y en la gestión de riesgos bajo la norma ISO9001:2015, se articula con el Plan Estratégico de Tecnología de la Información y Comunicaciones (PETI) del Sector Defensa**.** El PETI, a su vez, responde a la necesidad de actualizar y modernizar nuestros sistemas de información, telecomunicaciones y hardware, y fortalecer las áreas de Tecnología en las entidades del Sector. De esta manera, ambos planes convergen en el objetivo de resaltar las capacidades institucionales y sectoriales a través de la adopción de nuevas tecnologías y la implementación de medidas de seguridad de la información.

El Plan Estratégico de Tecnología de la Información y Comunicaciones (PETI) del Sector Defensa marca un hito en la transformación digital del Sector, siendo la seguridad de la información un pilar fundamental para su éxito**.** Esta integración permite fortalecer las capacidades institucionales y sectoriales, al tiempo que se fomenta la adopción de nuevas tecnologías y la mejora de la capacidad de respuesta ante amenazas y riesgos.

La necesidad de actualizar y modernizar nuestros sistemas de información, en la Dirección General de Sanidad Militar, ha dado lugar al Plan Estratégico de Tecnología de la Información y Comunicaciones (PETI) del Sector Defensa. Sin embargo, esta transformación digital debe ir acompañada de sólidas medidas de seguridad de la información**.** Dentro de nuestra institución se desarrolla un Modelo de Seguridad y Privacidad de la Información**,** el cual, en conjunto con el PETI, busca garantizar la protección de los activos de la información y la continuidad de los servicios**.** De esta manera, se logra una visión integral que abarca tanto la innovación tecnológica como la gestión de riesgos.

2. OBJETIVO GENERAL

Garantizar la integridad, confidencialidad y disponibilidad de los activos de información de la Dirección General de Sanidad Militar – DIGSA, implementando controles que permitan la mitigación de los riesgos a los cuales la entidad está expuesta, de acuerdo a los factores de exposición internos y externos, con el fin de mantener la protección de sus datos y continuidad de los servicios.

2.1. Objetivos Específicos

1. Elevar el nivel de madurez consolidando la posición de la Dirección General de Sanidad Militar con prácticas de seguridad de la información sólidas y actualizadas.

2. Proteger la información garantizando los principios de la confidencialidad, integridad y disponibilidad de los datos de la entidad, lineados con las políticas y procedimientos establecidos para la gestión del Sistema de Gestión y Seguridad de la Información.
3. Gestionar riesgos Identificando, evaluando y mitigando de manera proactiva los riesgos que puedan comprometer la seguridad de la información.
4. Integrar de manera efectiva las medidas de seguridad en todas las operaciones administrativas y logísticas, optimizando los procesos y garantizando la continuidad del servicio en toda la Dirección General de Sanidad Militar de una forma más eficiente y eficaz.

3. ALCANCE

El alcance del Modelo de Seguridad y Privacidad de la Información en la Dirección General de Sanidad Militar aplica a todos los activos de Información y al modelo de operación por procesos, siendo de obligatorio cumplimiento por parte de todos los funcionarios, contratistas y terceras partes que presten sus servicios a la misma. Inicia con una etapa de Diagnostico hasta la ejecución del ciclo PHVA en la fase de mantenimiento y mejora del Modelo de Seguridad y Privacidad de la Información y termina con el seguimiento al plan de trabajo del Modelo.

4. APLICACIÓN

- DIGSA, DISAN/JEFSA

5. FUNDAMENTO NORMATIVO

Proveedor	Entrada - insumo
Ley 44 de 1993	Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
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 1266 de 2008	Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1474 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Ley 1712 de 2012	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 1008 del 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 Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Proveedor	Entrada - insumo
Decreto 767 de 2022	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 Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
Resolución 1519 de 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Resolución 746 de 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021.
Resolución 7870 de 2022	Por la cual se emite y adopta la política General de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa.
Resolución 02277 de 2025	Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
Lineamiento MSPI	Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas
Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7	Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7 Departamento Administrativo de la Función Pública. 2025.

6. DEFINICIONES

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

Activos de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura.

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

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo.

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento.

Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

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

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 Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.

Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional: Información pública clasificada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley.

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.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital.

Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

7. ACRÓNIMOS

ARECO:	Área de Infraestructura Tecnológica, Redes y Comunicaciones
AREIN:	Área de Seguridad de la Información
ARIBD:	Área de administración del Sistema y Base de Datos
CCI:	Infraestructura Critica Cibernética.
IGSA:	Dirección General de Sanidad Militar.
MSPI:	Modelo de Seguridad y Privacidad de la Información.
SGSI:	Sistema de Gestión de Seguridad de la Información.
SISAM:	Grupo Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones

8. POLITICAS DE OPERACION

1. Política de Control de Acceso

Se establecerán mecanismos de autenticación y autorización para garantizar que solo el personal autorizado acceda a los activos de información, según sus funciones y niveles de responsabilidad.

2. Política de Clasificación y Manejo de la Información

Toda la información será clasificada según su nivel de sensibilidad (confidencial, restringida, pública) y tratada conforme a procedimientos definidos para su almacenamiento, transmisión y eliminación segura.

3. Política de Gestión de Riesgos

Se implementará un proceso continuo de identificación, análisis, evaluación y tratamiento de riesgos, considerando factores internos y externos que puedan afectar la integridad, confidencialidad y disponibilidad de la información.

4. Política de Continuidad del Servicio

Se desarrollarán planes de continuidad de negocio y recuperación ante desastres para asegurar la disponibilidad de los servicios críticos en caso de incidentes que afecten la operación normal.

5. Política de Seguridad Física y Ambiental

Se establecerán controles físicos para proteger los equipos, instalaciones y medios de almacenamiento contra accesos no autorizados, daños o interferencias.

6. Política de Seguridad en el Uso de Tecnologías de la Información

El uso de sistemas, redes y dispositivos estará regulado por normas que promuevan buenas prácticas, incluyendo actualizaciones periódicas, uso de antivirus, y restricciones en el uso de software no autorizado.

7. Política de Concientización y Capacitación

Todo el personal será capacitado regularmente en temas de seguridad de la información, incluyendo el manejo adecuado de datos, identificación de amenazas y respuesta ante incidentes.

8. Política de Monitoreo y Auditoría

Se realizarán actividades de monitoreo, revisión y auditoría para verificar el cumplimiento de las políticas, detectar vulnerabilidades y mejorar continuamente los controles implementados.

9. Política de Gestión de Incidentes de Seguridad

Se establecerá un protocolo para la detección, reporte, análisis y respuesta ante incidentes de seguridad, con el fin de minimizar su impacto y prevenir recurrencias.

10. Política de Cumplimiento Normativo

Se garantizará el cumplimiento de las leyes, regulaciones y estándares aplicables en materia de seguridad de la información, incluyendo normativas nacionales e internacionales.

9. EJECUCIÓN

9.1. Proceso de Seguridad y Privacidad de la Información

La Dirección General de Sanidad Militar (DIGSA) tiene como objetivo evaluar el grado de cumplimiento de los requerimientos del Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Para ello, se implementará un ciclo de mejora continua PHVA (Planificar-Hacer-Verificar-Actuar) alineado con las fases del Modelo de Seguridad y Privacidad.

Con el fin de salvaguardar la información crítica de la Dirección General de Sanidad Militar, El Oficial de Seguridad de la Información (OSI) de la DIGSA, se encarga de la detección temprana, respuesta y recuperación ante incidentes cibernéticos en el centro de monitoreo SOC - NOC de la entidad. Así mismo, lidera la implementación y mejora continua del Modelo de Seguridad y Privacidad de la Información, asegurando el cumplimiento de los estándares más altos en materia de ciberseguridad teniendo en cuenta que tiene asignada unas tareas así:

Responsabilidades del OSI:

1. Gestión del Centro de Operaciones de Seguridad (SOC) y de Redes (NOC)

   - Monitoreo constante de los sistemas y redes de la entidad en busca de amenazas y anomalías.

- Detección temprana de incidentes de seguridad.
- Análisis forense de incidentes para determinar su origen y alcance.
- Respuesta rápida y eficaz a los incidentes cibernéticos.
- Coordinación con los equipos técnicos y de negocio durante y después de un incidente.
- Implementación de medidas correctivas para prevenir la recurrencia de incidentes.

2. Liderazgo en la implementación y mejora del Modelo de Seguridad y Privacidad

- Diseño, implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información de la DIGSA.
- Asegurar la alineación del modelo con los estándares y regulaciones nacionales e internacionales en materia de ciberseguridad.
- Realización de evaluaciones de riesgo periódicas para identificar y mitigar las amenazas.
- Desarrollo e implementación de políticas y procedimientos de seguridad.
- Concientización y capacitación del personal en temas de seguridad de la información.

3. Cumplimiento Normativo

- Asegurar el cumplimiento de las leyes y regulaciones aplicables en materia de protección de datos y seguridad de la información.
- Gestión de auditorías y certificaciones de seguridad.

4. Relaciones Externas

- Colaboración con proveedores de servicios de seguridad.
- Participación en comunidades de seguridad de la información.
- Mantenerse actualizado sobre las últimas tendencias y amenazas en ciberseguridad.

a. Perfil del OSI

1. Conocimientos técnicos

- Sólidos conocimientos en redes, sistemas operativos, seguridad de la información y tecnologías de la información.
- Experiencia en herramientas de seguridad como firewalls, sistemas de detección de intrusiones, sistemas de prevención de pérdida de datos, etc.
- Conocimiento de estándares y marcos de trabajo de seguridad como ISO 27001, NIST Cybersecurity Framework, etc.

2. Habilidades

- Pensamiento analítico y capacidad para resolver problemas complejos.
- Habilidades de liderazgo y gestión de equipos.
- Habilidades de comunicación efectiva, tanto verbal como escrita.
- Capacidad para trabajar bajo presión y gestionar múltiples tareas simultáneamente.
- Orientación a resultados y proactividad.

3. Experiencia

- Experiencia previa en roles similares, preferiblemente en entornos altamente regulados.
- Experiencia en la gestión de incidentes de seguridad.
- Conocimiento de las mejores prácticas en seguridad de la información.

El OSI de la DIGSA es un profesional clave responsable de garantizar la seguridad de la información de la entidad. Su rol abarca desde la detección y respuesta a incidentes cibernéticos hasta el diseño y la implementación de un sólido marco de seguridad.

Trabajo del OSI de la DIGSA es un proceso continuo y evolutivo. A través de la aplicación del ciclo PHVA, el OSI planifica, implementa, verifica y mejora las medidas de seguridad de la información de manera cíclica. Desde la detección y respuesta a incidentes hasta la evaluación de riesgos, el OSI asegura que la DIGSA esté siempre un paso adelante de las amenazas cibernéticas

El OSI de la DIGSA desempeña un papel crucial en la protección de los activos de información de la entidad. Al liderar la implementación y mejora continua del Modelo de Seguridad y Privacidad de la Información, basado en el ciclo PHVA de seguridad y privacidad de la información el OSI garantiza que la DIGSA esté siempre preparada para enfrentar los desafíos cibernéticos actuales así:

Planear

- Realizar el autodiagnóstico del MSPI
- Definir la política de seguridad integral.
- Realizar el Inventario detallado de activos de información y tecnológicos.
- Identificar, analizar y evaluar las posibles amenazas y vulnerabilidades.
- Socializar el Modelo de Seguridad y Privacidad de la información apoyado en todo el personal de la entidad a través de difusiones de boletines de seguridad digital por el correo institucional, charlas, fondos de pantalla, Tips de seguridad digital en las órdenes del día, entre otros.

Hacer

- Desarrollar y ejecutar programas de sensibilización para todo el personal.
- Diseñar y ejecutar un plan de tratamiento de riesgos, incluyendo la definición y aplicación de controles de seguridad adecuados.

Verificar

- Realizar auditorías internas periódicas para evaluar el Sistema de Gestión de Seguridad de la Información (SGSI).
- Medir la eficacia de los controles implementados.

Actuar

- Implementar de acciones correctivas y preventivas para cerrar brechas de seguridad.
- Verificar la efectividad de las medidas implementadas.

A través de este ciclo PHVA, DIGSA busca establecer una base sólida para la gestión de la seguridad y privacidad de la información, garantizando la protección de los activos de información y el cumplimiento de los estándares establecidos por el MinTIC.

9.2. Análisis del Contexto Interno y Externo

ENTORNO INTERNO	
FORTALEZAS	DEBILIDADES
F1. Talento Humano fortalecido, con capacidades y competencias en la gestión de servicios TI, Infraestructura y gestión de riesgos de seguridad Informática y Seguridad de la Información, soporte TI. F2. Seguridad de la Información: Fortalecimiento de la seguridad y privacidad de la información mediante la implementación de herramientas tecnológicas que permiten la detección de vulnerabilidades y amenazas contra los sistemas información y la infraestructura TI, compuesto por los siguientes elementos: - Implementación de un sistema de seguridad firewall.; - Implementación de un Sistema de seguridad de análisis de vulnerabilidades de Seguridad de la información (SOC).; - Implementación de un Sistema de Seguridad de redes (NOC).; - Implementación de doble factor de autenticación (accesos a cuentas, sistemas de información, dispositivos.; - ; - Capacitación continua al personal en criterios de seguridad de la información y ciberseguridad. F3. Infraestructura Tecnológica: Renovación y actualización de infraestructura tecnológica de comunicaciones, servidores, redes, equipos de almacenamiento.; - Gestión y administración continua de infraestructura TI.; Disponer de infraestructura TI que soporta los procesos. F4. Sistemas de Información y Base de Datos: Actualización continua del Sistema de Información SALUD.SIS a través del contrato Fabrica de Software.; - Implementación de lineamientos y procedimientos para la gestión y control de cambios TI.; - Análisis y evaluación de sistema de información y requerimientos. F5. Implementación criterios de Política de Gobierno Digital y Modelo de Gobierno y Gestión TI. Política de Seguridad de la Información, el Manual de Políticas.	D1. Limitado recurso humano para el cumplimiento del Objetivo y alcance del Proceso. D2. Desactualización del Sistema de Gestión (Caracterización, Procedimientos, Políticas, Manuales). D3. Limitado presupuesto para la reposición, actualización de Equipos Comunicaciones, Computo. D4. Falta de Integración de los Sistemas de Información. D5. Limitada capacidad de recursos humano para la Implementación del Modelo Seguridad de la Información, Marco de Arquitectura Empresaria, Transformación Digital. D6. Dependencia Administración de Sistemas de Información Comando General (Gestión Documental y SUITE VISION). D7. Bajo uso y apropiación de los servicios TI (APP Mesa de Ayuda, Intranet). D8. Falta de licenciamiento de herramienta de mesa de servicios para TI con ANS. D9. Falta de dotación de equipos para soporte y mantenimiento Correctivo de TI. D10. Falta de Madurez y estabilización del Sistema de Información SALUD.SIS. D11. Limitada Planificación Presupuesto TI. D12. Fuga de Conocimiento. D13. Falla Acuerdos de Servicios Proveedores. D14. Fallas técnicas de los Sistemas de información y Base de Datos. D15. Perdida de la Información por fallas tecnológicas y recurso humano. D16. Falta de sensibilización y concientización por parte de los funcionarios de la DIGSA en lo referente en la Seguridad de la Información, falta de compromiso de los funcionarios para capacitarse.

ENTORNO EXTERNO	
OPORTUNIDADES	AMENAZAS
O1. Acompañamiento Min Tic Política de Seguridad de Información, Modelo de Seguridad Privacidad de Información, Transformación Digital. O2. Capacitación en herramientas Ofimáticas como apoyo a la gestión. O3. Implementación de herramientas para la identificación de vulnerabilidades. O4. Herramienta para el Análisis y evaluación de necesidades TI. O5. Implementación buenas prácticas entidades del sector modelo de seguridad y privacidad de la información. O6. Gestión y Planificación Presupuesto TI. O7. Implementaciones nuevas tecnologías y tendencias TI. O8. Capacitación en Gestión y Administración TI, con entidades externas como MINTIC. O9. Capacitación y Transferencia de Conocimiento, desde los proveedores O10. Disponibilidad de Consultoría Fabrica de Software. 011. Mesas de ayuda con CCOCI y COMJ6, con los contratos relacionados con seguridad de la información,	A1. Pérdida, hurto, fuga, destrucción y/o desviación de la información por Ataques Cibernéticos, accesos no autorizados de usuarios, desastres o eventos fortuitos. A2. Fuga de Información por acceso no autorizados. A3. Perdida en la Continuidad del Negocio debido a fallas en infraestructura TI, Sistema de Información, Comunicaciones y Seguridad de la Información. A4. Cambios Tecnológicos Acelerados. A5. Recortes presupuestales Gestión TI. A6. Incumplimiento ANS Proveedores. A7. Cambios Normativos. A8. Falla Equipos de Comunicación y Servicios TI Proveedores A9. Falla servicios canales de comunicación. A10. Ataques cibernéticos a los proveedores, generando perdida de la información de la entidad.

ENTORNO EXTERNO	
OPORTUNIDADES	AMENAZAS
Infraestructura y Bases de Datos, en ocurrencia a incidentes presentados. O12. Apoyo del Sector Defensa (Comando Conjunto Cibernético) en la gestión de identificación de vulnerabilidades y amenazadas que afecten la integridad de la Seguridad de la Información.	

Estrategias DOFA

ESTRATEGIAS (DO)	ESTRATEGIAS (DA)
D1O2O8O9 Fortalecer el desarrollo de programas de capacitación herramientas TI, Gestión TI, y en la gestión de áreas critica TI, para garantizar la continuidad de servicios de TI y Sistema de Información, con la posibilidad de fortalecer el recurso humano. O10D3D9D11D14 Optimizar el uso de presupuesto mediante la priorización de inversiones en tecnologías de protección critica, asegurando que los recursos se enfoquen en las áreas más vulnerables y estratégicas de la DIGSA. D15D16O9011O12 Optimizar los procesos de respaldo y recuperación de información, mediante la implementación de copias de seguridad automatizadas o manual en diferentes ubicaciones (servidores locales y en la nube), garantizando que los datos críticos siempre estén disponibles. Además, establecer planes de contingencia y pruebas periódicas de restauración. D2D5D15D16O1O2O3O4O5O9O13 Actualizar, desplegar las políticas de seguridad y privacidad de la Información y Ciberseguridad con estándares de Comando Conjunto Cibernético CCOCI y Ministerio de Tecnologías de la Información y Comunicaciones MINTIC, asegurando su aplicación efectiva en todas las áreas de la DIGSA. D2D7D12D13D14O2O8O12 Actualización Procedimientos, Políticas y Manuales acorde a los estándares mínimos establecidos por la Política de Gobierno Digital en sus dominios de Seguridad y Privacidad de la Información y Transformación Digital. D3O7O8 Priorización de recursos de inversión para la actualización, reposición de infraestructura TI. D10O14 Revisión, análisis de requerimientos técnicos y funcionales a cargo del Equipo Táctico del Sistema de Información SALUD.SIS, con el apoyo del Equipo Funcional - Operativo del Sistema de Información SALUD.SIS, que permita la estabilización y escalabilidad del SI. D5O9010 Garantizar la continuidad a la contratación de expertos para asegurar la implementación de la Política de Gobierno Digital e Implementación de necesidades tecnología a nivel de infraestructura TI y Sistemas de Información. D6O11014 Evaluar alternativas de Tecnología y Sistema de Información que integren las necesidades de Suit Visión y Gestión Documental, con el objetivo reducir la dependencia de sistemas externos y tener una gestión operativa. D70602 Desarrollar programas de capacitación y sensibilización para el uso de aplicaciones Office 365, mesa de ayuda e intranet, con el objetivo de mejorar la productividad y el uso de servicios TI	D1A1 Capacitar a los funcionarios en políticas de seguridad y privacidad de la información, Ciberataques, prevención de riesgos, adopción de buenas prácticas gestión de usuarios, roles y perfiles. D2A1 Revisión y actualización del sistema de gestión en sus componentes de Matriz DOFA, Caracterización, Procedimientos, Políticas y Manuales, alineados a la Guía del Modelo y Seguridad de la Información Política de Gobierno Digital de Min Tic. D3D8D14A1A3A4 Realizar Inventario de Infraestructura TI, Sistemas de Información, Servidores, Equipos de Comunicaciones, priorizando la adquisición, reposición, con el fin de garantizar la continuidad del negocio y servicios. D4A4 Desarrollar estrategias de integración de Sistemas de Información misionales, Administrativos y de apoyo, garantizando el flujo, flexibilidad y gestión de la información. A1A2A3A9D15D16Garantizar la continuidad de los servicios de seguridad de informática, mediante la contratación de proveedores especializados, que apoyen la protección de la infraestructura y sistemas de información de posibles ciberataques. A2A6D13D14Establecer cláusulas de protección de datos personales con los proveedores en los procesos de contratación, asegurando que cumplan con los criterios de confidencialidad. A1A2A3D5Realizar la contratación de expertos que permitan avanzar en la implementación de la Política de Gobierno Digital e Implementación de necesidades tecnología a nivel de infraestructura TI y Sistemas de Información. A6D13Realizar la plantificación y seguimiento a los acuerdos de servicios ANS de acuerdo a los criterios establecidos en el proceso de contratación y ejecutar acciones frente a posibles incumplimientos. A3A7D10Realizar evaluación del grado de madurez del Sistema de Información SALUD.SIS de acuerdo los criterios técnicos y funcionales que se requieren normativamente y institucionalmente, revisando dentro del Equipo Táctico del Sistema de Información SALUD.SIS para su aprobación, desarrollo, implementación y puesta en marca, garantizando la estabilización y escalabilidad SI

ESTRATEGIAS (FO)	ESTRATEGIAS (FA)
F1O12 Realizar transferencia de Conocimiento Lideres y Responsables procesos Críticos TI. Generando compromiso Institucional con la mejora continua de la resiliencia cibernética. F1O2 Gestionar Capacitaciones con Min Tic para el fortalecimiento en Seguridad de Información, Modelo de Seguridad Privacidad de Información, Transformación Digital en las plataformas dispuestas para el fortalecimiento de habilidades digitales. Implementar programas de formación continua para mejorar la apropiación tecnológica. F2O1O409 Actualización y mejora continua en la implementación de herramientas para el monitoreo, análisis de vulnerabilidades y seguridad de redes. Apoyado con entidades del sector que permitan la mejora en la inteligencia y detección de amenazas, vulnerabilidades fortaleciendo la seguridad perimetral, protección de infraestructura critica, activos de información, Priorizando la automatización de procesos críticos y la integración de sistemas para mitigar riesgos operativos. F1O3O6 Brindar actualización a usuarios en la gestión y aplicación de herramientas ofimáticas para el fortalecimiento y apoyo de procesos. F4O14 Identificar las necesidades y requerimientos para la estabilización del Sistema de Información SALUD.SIS, realizar evaluación de la tasa de uso del sistema de información. F3O10O11 Actualización y mejora continua de la infraestructura TI, nuevas tecnologías emergentes y tendencias, soportado en planificación TI a corto, mediano plazo, mediante el análisis y evaluación TI para la gestión de recursos propios y proyectos de inversión. F5O2 Avanzar en la implementación del Política de Gobierno Digital y el Dominio del Modelo de Gestión y Gobierno TI, Modelo de Seguridad y Privacidad de la Información, Plan de Transformación Digital, mediante alianzas estratégicas con entidades del Sector y acompañamiento de Min Tic.	F1F2F3F5A1A2A3 Implementar un programa continuo de concienciación, capacitación en ciberseguridad, ciberseguridad, gestión de riesgos, fuga de información para personal militar y administrativo, enfocándose en protocolos de seguridad, identificación de phishing y protección de información confidencial. F1F2F3F5A1A2A3 Implementar procedimientos de auditoria y verificación constante en la seguridad de la información, asegurando el cumplimiento de normativas y detectando posibles fallos en la infraestructura tecnológica. F1F2F3F5A1A2A3 Fortalecer el control de dispositivos de almacenamiento externos mediante políticas estrictas de acceso y cifrado automático, evitando la extracción no autorizada de información sensible. F1F2F4F5A1A2A3A10 Fortalecer la capacidad de respuesta ante factores de riesgos, mejorando la continuidad del negocio, mediante la aplicación de herramientas, infraestructura, y procedimientos establecidos. F1F3A4A5A6 Realizar la identificación necesidades de infraestructura TI, Sistemas y Tecnologías Emergentes para gestión de recursos propios y/o a través de proyectos de inversión, que permitan la actualización, renovación tecnológica de la infraestructura, redes, servidores, equipos de almacenamiento que soporte los cambios tecnológicos y demás de los procesos. F1F5A7 Actualización continua en cambios normativos para la implementación y adopción de lineamientos Política Gobierno Digital. A6A8A9F1F2F3F4 Seguimiento al cumplimiento de acuerdos de servicios ANS mediante indicador de eficiencia que permita alertar sobre posibles fallos o incumplimiento de los ANS acordados dentro del procesos contractuales.

10. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La DIRECCION GENERAL DE SANIDAD MILITAR DIGSA entendiendo la importancia de la adecuada gestión de la información, está comprometida con la implementación del sistema de seguridad de la información, implementando estrategias y herramientas acorde a los lineamientos establecidos por el Ministerio TICS y de acuerdo con su misión y visión institucional.

Para la DIGSA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, y **p**ara asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Cumplir con los principios de seguridad de la información.
- Mantener la confianza con los actores del ciclo de operación.

- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, usuarios, proveedores y clientes.

Esta política aplica a los funcionarios, contratistas y terceros de toda la entidad.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación, se establecen las políticas que la DIRECCION GENERAL DE SANIDAD MILITAR DIGSA establece en el marco Sistema de Gestión de Seguridad de la Información – SGSI.

La **DIRECCION GENERAL DE SANIDAD MILITAR DIGSA**, ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información.

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

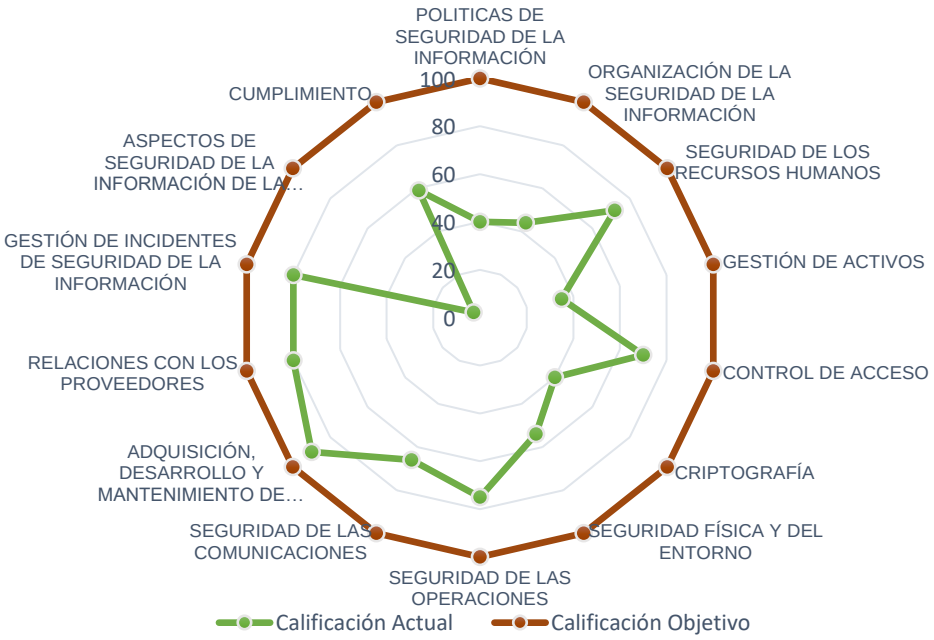
- Protegerá la información generada, procesada o resguardada por los procesos y activos de información que hacen parte de estos.
- Protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- Protegerá su información de las amenazas originadas por parte de sus funcionarios, clientes y proveedores.
- Protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementará control de acceso a la información, sistemas y recursos de red.
- Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- Garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- Garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

11. AUTODIAGNOSTICO ESTADO ACTUAL MSPI.

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.

1. Autodiagnóstico Estado Actual DIGSA



Fuente: Grupo SISAM – Área Seguridad de la Información AREIN.

Tabla 1 Evaluación de Efectividad de controles

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS 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

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
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: Grupo SISAM – Área Seguridad de la Información AREIN.

El Grupo de Gestión de la Información y las Comunicaciones realizar la implementación del Documento Maestro del Modelo de Seguridad y Privacidad de la Información Versión 5 2025, realizando la actualización del autodiagnóstico acorde a la norma 27001:2022 que soporta MSPI, para lo cual en el primer semestre 2026 implementará el autodiagnóstico lo que permitirá establecer una hoja de ruta para su despliegue en las vigencias 2027 – 2030.

12. ESTRATEGIA SEGURIDAD DE LA INFORMACION

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la normatividad vigente:

Tabla 2. Estratégicas y Ejes

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

Fuente: Grupo SISAM – Área Seguridad de la Información AREIN.

13. ACTIVIDADES A DESARROLLAR

Tabla 3. Cronograma de Actividades a Desarrollar 2026

					Fecha Programada	
Ejes	**Gestión**	**Actividades**	**Producto**	**Responsable**	**Fecha Inicial**	**Fecha Final**
Fortalecimiento del MSPI	Actualizar el autodiagnóstico del MSPI	Aplicar la herramienta Min Tic 2025 para el autodiagnóstico del MSPI	Informe estado actual MSPI DIGSA	Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones SISAM Coordinaciones DIGSA	02/01/2026	30/04/2026
	Manual del Modelo se Seguridad y Privacidad de la Información MSPI DIGSA	Actualizar el Modelo de Seguridad y Privacidad de la Información DIGSA	Manual de Modelo de Seguridad y Privacidad de la Información DIGSA	Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones SISAM	02/01/2026	30/05/2026
	Actualizar el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética	Realizar la actualización de la matriz de activos de información e infraestructura critica Cibernética.	Matriz de activos de información e infraestructura critica Cibernética.	Área Seguridad de la Información- AREIN – Grupo SISAM.	02/01/2026	31/03/2026
	Actualización Matriz de Riesgos Seguridad y Privacidad de la Información, Seguridad Digital y continuidad del negocio.	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad del negocio.	Matriz de Riesgos Actualizada	Área Seguridad de la Información- AREIN – Grupo SISAM.	02/01/2026	31/03/2026

					Fecha Programada	
Ejes	**Gestión**	**Actividades**	**Producto**	**Responsable**	**Fecha Inicial**	**Fecha Final**
	Actualizar la Política General de Seguridad de la Información	Revisión criterios MSPI y actualización Política General de Seguridad de la Información.	Política General de Seguridad de la Información	Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones SISAM Grupo Gestión de la Información – GRUGI	02/01/2026	31/03/2026
	Manual de políticas del MSPI	Actualizar el Manual de políticas del MSPI	Manual de Políticas del MSPI DIGSA	Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones SISAM Grupo Gestión de la Información – GRUGI	02/01/2026	31/03/2026
Gestión MSPI	Monitoreo Riesgo Seguridad y Privacidad de la Información, Seguridad Digital y continuidad del negocio	Realizar monitoreo trimestrales Matriz de Riesgos Seguridad y Privacidad de la Información, Seguridad Digital y continuidad del negocio	Informe monitoreo Riesgos	Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones SISAM Grupo Gestión de la Información – GRUGI	02/01/2026 01/04/2026 01/07/2026 01/10/2026	31/03/2026 30/06/2026 30/09/2026 22/12/2026
	Incidentes de Seguridad y Privacidad de la Información	Realizar seguimiento a los Incidentes de Seguridad y Privacidad de la Información	Tablero Control Indicadores	Área Seguridad de la Información- AREIN – Grupo SISAM. Área Infraestructura, Redes y Comunicaciones – ARECO. Área Administración del Sistema y Base de Datos - ARIBD	02/01/2026 01/04/2026 01/07/2026 01/10/2026	31/03/2026 30/06/2026 30/09/2026 22/12/2026
	Seguimiento a vulnerabilidades	Detectar a través de un software actividades sospechosas	Informe de Mitigación vulnerabilidades y alertas de seguridad detectadas.	Área Seguridad de la Información- AREIN	02/01/2026 01/04/2026 01/07/2026 01/10/2026	31/03/2026 30/06/2026 30/09/2026 22/12/2026
Uso y Apropiación MSPI	Capacitar al personal de la DIGSA	Realizar jornadas de sensibilización Políticas, Riesgos y buenas prácticas.	Acta de Capacitación Seguridad y Privacidad de la Información	Área Seguridad de la Información- AREIN	01/04/2026 01/10/2026	30/06/2026 22/12/2026

Fuente: Grupo SISAM – Área Seguridad de la Información AREIN.

14. PROYECTOS CONTRACTUALES

De acuerdo con las actividades en la estrategia de Seguridad de Información, la Dirección General de Sanidad Militar DIGSA, tiene recursos asignados para el fortalecimiento de controles que permitan la mitigación de riesgos de Seguridad y Privacidad de la información, de acuerdo a los factores internos y externos, a continuación, se presenta el presupuesto que soporta las actividades de permiten la mitigación de riesgos de Seguridad y Privacidad de la información.

Tabla 4. Proyectos contractuales

Proyecto	**Objetivo**	**Alcance**	Presupuesto
La Dirección General de Sanidad Militar requiere renovar la garantía y soporte de sus servidores para asegurar la continuidad operativa de sus sistemas críticos. Esta renovación garantiza disponibilidad del 99.98%, protección ante fallos de hardware, acceso prioritario a soporte técnico, y evita costos inesperados, permitiendo una gestión eficiente y segura de la infraestructura tecnológica institucional.	Garantizar el servicio de renovación de garantía y soporte de servidores asegurando que la infraestructura tecnológica de la Dirección General de Sanidad Militar se mantenga en condiciones óptimas. Al actualizar garantías y proporcionar soporte técnico continuo, se mejora la fiabilidad y el rendimiento de los servidores, lo que fortalece la estabilidad y la eficiencia de toda la infraestructura tecnológica. Esta actualización no solo previene fallos y prolonga la vida útil de los activos informáticos, sino que también asegura un funcionamiento más seguro y eficiente, beneficiando así la operación y la gestión tecnológica de la DIGSA, aplicando las buenas prácticas que están alineadas a la ISO 27001.	El alcance del servicio de renovación de garantía y soporte de servidores contempla la mejora continua de la infraestructura tecnológica de la Dirección General de Sanidad Militar. Mediante la actualización de garantías y la provisión de soporte técnico especializado, se asegura el mantenimiento preventivo y correctivo de los servidores, lo que se traduce en un rendimiento más estable y confiable. Este enfoque proactivo permite minimizar los riesgos de fallos, prolongar la vida útil de los equipos y garantizar una operación ininterrumpida de los sistemas críticos. Como resultado, la DIGSA experimentará una mayor eficiencia operativa, un fortalecimiento de la seguridad de la información y una infraestructura tecnológica más robusta y resiliente.	$ 72.588.800
Mantenimiento, Soporte, Actualización y solución para los Firewall de la DIGSA, Ministerio de Defensa Nacional (Edificio Fortaleza), XDR y suscripción del servicio de protección de correo electrónico (FortiMail) de la Dirección General de Sanidad Militar.	Llevar a cabo el mantenimiento, soporte, actualización y solución de problemas para los firewalls de la DIGSA y el Ministerio de Defensa Nacional (Edificio Fortaleza), así como el XDR y el servicio FortiMail de la Dirección General de Sanidad Militar, es asegurar una defensa cibernética sólida y continua. Esta gestión integral mejorará la protección contra ciber amenazas, mantendrá la integridad y confidencialidad de la información y optimizará la seguridad general de la	La gestion integral de los firewalls de la Dirección General de Sanidad Militar (DIGSA) y del Ministerio de Defensa Nacional (Edificio Fortaleza), así como del sistema de detección y respuesta extendida (XDR) y del servicio de protección de correo electrónico FortiMail, constituye una acción estratégica para fortalecer la seguridad de la red y los sistemas institucionales. La ejecución continua de actividades de mantenimiento, soporte, actualización y	$ 750.000.002,64

Proyecto	Objetivo	Alcance	Presupuesto
	infraestructura tecnológica. Con estos servicios, la DIGSA logrará una mayor estabilidad operativa, reducirá vulnerabilidades y garantizará un entorno tecnológico más seguro y eficiente.	resolución de incidencias garantiza una protección robusta frente a amenazas cibernéticas, preserva la integridad y confidencialidad de la información, y contribuye a un funcionamiento seguro y eficiente de la infraestructura tecnológica de la DIGSA.	
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.	Suministrar y gestionar switches, puntos de acceso, servicios SOC y NOC, administración y seguridad SOC, así como la renovación de certificados SSL, es optimizar la infraestructura de telecomunicaciones de la Dirección General de Sanidad Militar. Al instalar y configurar estos componentes, junto con la implementación de los centros de operaciones de red (NOC) y seguridad (SOC), se mejorará significativamente la eficiencia y la seguridad de la red. Esto asegura una gestión más efectiva de la red y la protección de datos, reduciendo vulnerabilidades y fortaleciendo la capacidad operativa general de la DIGSA.	El suministro y gestión de la adquisición de switches, puntos de acceso, servicios SOC y NOC, así como la renovación de certificados SSL, e instalar y configurar la infraestructura de telecomunicaciones, incluye la implementación de centros de operaciones de red (NOC) y de seguridad (SOC). Esto impactará positivamente al mejorar la eficiencia y seguridad de la red en la Dirección General de Sanidad Militar. Con una infraestructura bien establecida y servicios operativos de monitoreo y protección, se logrará una gestión más eficaz de la red, una mayor seguridad de los datos y una reducción de vulnerabilidades, optimizando la operatividad tecnológica de la DIGSA.	$ 1.205.518.293.63
Adquisición de licencias (Single Sign on AZURE-DEVOPS) y renovación del servicio por suscripción licenciamiento Microsoft mediante acuerdo marco de precios del instrumento de agregación de demanda software por catálogo para la Dirección General de Sanidad Militar.	Adquirir y renovar licencias de Microsoft a través del acuerdo marco de precios y el instrumento de agregación de demanda, es mejorar la gestión de software en la Dirección General de Sanidad Militar. Este enfoque garantiza el acceso continuo a versiones actualizadas y soporte técnico eficiente, lo que optimiza el funcionamiento de las herramientas tecnológicas y asegura la conformidad con las normativas de licenciamiento. Con esta renovación, se reducen riesgos relacionados con software desactualizado, se mejora la eficiencia operativa y se mantiene un entorno tecnológico seguro y fiable, beneficiando el	Asegurar acceso continuo a versiones actualizadas y soporte técnico, optimizando el rendimiento de las aplicaciones y reduciendo riesgos asociados con el uso de software obsoleto o sin licencia. Al garantizar un suministro estable y regulado de licencias, se incrementa la eficiencia operativa y se asegura el cumplimiento normativo, fortaleciendo la infraestructura tecnológica y contribuyendo un entorno de trabajo más seguro y productivo	$ 711.614.076,24

Proyecto	Objetivo	Alcance	Presupuesto
	desempeño general de la DIGSA.		

Fuente: Grupo SISAM – Área Seguridad de la Información AREIN.

15. MONITOREO Y REVISIÓN DEL PLAN

Para contribuir con el logro de los objetivos, interesándose por el monitoreo y seguimiento periódico de los riesgos (impactos, amenazas, vulnerabilidades y probabilidades), en busca de posibles cambios que requieran la valoración; esta acción debe ser realizada en concordancia con la Política de Evaluación de Resultados y la Política de control interno para lo cual se debe tener en cuenta el despliegue del siguiente Esquema de Líneas De Defensa:

Tabla 5. Esquemas de Líneas de Defensa de la DIGSA

Líneas de Defensa	Responsable	Responsabilidad
Primera Línea	Coordinadores de Grupos, áreas y de equipo de trabajo de los procesos.	○ Es la gestión operativa y el control del día a día del Cronograma de actividades del Plan Institucional. ○ Realizar el seguimiento y la evaluación de los resultados institucionales de cada uno de los planes o programa a cargo. ○ Establecer oportunamente las acciones de corrección o prevención de riesgos asociados, si aplica, y registrar o suministrar los datos en los diferentes sistemas de información disponibles. ○ Revisar y actualizar los indicadores que establecen el grado de avance de los planes institucionales y demás mecanismos de seguimiento y evaluación establecidos. ○ Formular en periodos trimestrales el informe de seguimiento al cumplimiento de actividades del Cronograma de cada Plan Institucional a cargo y remitirlos al Grupo de Planeación Estratégica- MIPG.
Segunda Línea	Grupo de Planeación Estratégica-MIPG	○ Asesorar la formulación de los planes Institucionales en coordinación con los lineamientos establecidos en mesas de trabajo y políticas de líderes de políticas del nivel nacional ○ Liderar el seguimiento y la evaluación del cumplimiento al cronograma de cada uno de los Planes institucionales aprobados por el Comité de Gestión y desempeño Institucional. ○ Consolidar el informe de avance de la gestión y el desempeño institucional en los periodos establecidos.

Líneas de Defensa	Responsable	Responsabilidad
Tercera Línea	Grupo Seguimiento y Evaluación	○ Realizar evaluación independiente de las Políticas institucionales.

Fuente: Grupo SISAM – Área Seguridad de la Información AREIN.

- Por lo anterior cada líder de proceso, con su equipo de trabajo, deben verificar el desarrollo de las actividades, que ayudarán al cumplimiento de los objetivos institucionales, de forma periódica y en el cual deben participan personal militar o civil que dirigen y ejecutan los procesos, programas y/o proyectos, según el grado de responsabilidad y autoridad para su operación.

- El grupo de Planeación asesora la formulación de planes institucionales y convoca el comité de gestión y desempeño para la respectiva aprobación, y realizara la evaluación y seguimiento como segunda línea de defensa.

16. SEGUIMIENTO

Actualmente la entidad realiza seguimiento a través de nueve (9) indicadores que permiten medir, evaluar los criterios del marco de seguridad y privacidad de la información en lo referente a: disponibilidad, confidencialidad e integridad de los activos de información, a continuación, se presentan el tablero de indicadores implementado.

Tabla 6. Tablero de Indicadores

ID	TIPO	INDICADOR	%	FORMULA	VARIABLES	FRECUENCIA
1	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
2	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
3	Gestión	Porcentaje de implementación de controles	**PSI**	(VSI032/VSI33)*100	**VSI32:** Número de Controles Implementados **VSI33:** Número de Controles que se planearon implementar	Trimestral

ID	TIPO	INDICADOR	%	FORMULA	VARIABLES	FRECUENCIA
4	Gestión	Tratamientos de Eventos Relacionados en Marco de Seguridad y Privacidad de la Información	**TERSG**	(VSI05/VSI06)*100	**VSI05:** Número de anomalías cerradas. **VSI06:** Número total de anomalías encontradas.	Trimestral
5	Eficacia	Disponibilidad de Servicios TI (DSTI):	**DSTI**	((TSA-TB)/TSA)*100	Tiempo de servicio acordado (TSA): Es el tiempo total en el que el servicio debería estar disponible, según el plan de operaciones o el horario de funcionamiento esperado. Sumatoria de los tiempos sin servicio (TB): Se refiere al tiempo en que el servicio o sistema no está funcionando correctamente y accesible para los usuarios.	**Trimestral**
6	Eficacia	Índice de Incidentes de Seguridad (ISI):	**ISI**	(NIS/PT)	Número Total de Incidentes de Seguridad (NIS): Cantidad de eventos o incidentes de seguridad detectados durante un período específico. Esto puede incluir varios tipos de incidentes, como accesos no autorizados, violaciones de políticas de seguridad, fugas de datos, ataques cibernéticos, malware, etc. Periodo de Tiempo (PT): Es el intervalo en el cual se están midiendo los incidentes. Este período puede ser un mes, un trimestre, un semestre, o un año, depende de la frecuencia con la que se desea hacer el análisis.	**Trimestral**
7	Eficacia	Pérdida de Información por Ataques Cibernéticos (IPIA)	**IPIA**	(NIPIDCI/NTAC)*100	Número de incidentes de perdida de integridad, disponibilidad y confidencialidad de la información: Número de incidentes en los que se ha perdido o comprometido la integridad, disponibilidad y confidencialidad de la información debido a ataques cibernéticos. Número Total de ataques cibernéticos: Número total de ataques cibernéticos que	**Trimestral**

ID	TIPO	INDICADOR	%	FORMULA	VARIABLES	FRECUENCIA
					ocurrieron en el mismo período de tiempo (malware, phishing, ransomware, hackeo, ataques DDoS.	
8	Efectividad	Indicador de Pérdida de Confidencialidad de la Información por Gestión Inadecuada de Roles (IPCC)	**IPCC**	(NIPCGIR/NTIPC)*100	Número de incidentes de pérdida de confidencialidad debido a gestión inadecuada de roles (NIPCGIR): Es el número de incidentes en los que la pérdida de confidencialidad (es decir, la divulgación o exposición no autorizada de información sensible) ha ocurrido debido a una gestión incorrecta de roles y permisos. Número total de incidentes de pérdida de confidencialidad (NTIPC): Es el número total de incidentes de pérdida de confidencialidad que ocurren dentro de la organización.	**Trimestral**
9	Efectividad	Índice de Disponibilidad de Información Post-Desastre (IDIPD):	**IDIPD**	(NARSC/NTAAD)*100	Número de activos de información recuperados sin corrupción (sin pérdida de integridad) (NARSC): cantidad de activos de información (bases de datos, archivos, sistemas, etc.) que han sido recuperados con éxito después de un desastre o evento inesperado, y que no han sufrido alteraciones en su integridad. Número total de activos afectados por desastres o eventos fortuitos (NTAAD): Es la cantidad total de activos de información que han sido afectados por el desastre o evento inesperado, sin importar si fueron recuperados con éxito o no.	**Trimestral**

ID	TIPO	INDICADOR	%	FORMULA	VARIABLES	FRECUENCIA
10	Eficiencia	Disponibilidad de Sistemas de Información	**DSI**	DSI = ((TSA – TB) / TSA) *100	DSI = 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.	**Trimestral**

Fuente: Grupo SISAM – Área Seguridad de la Información AREIN.

De acuerdo al seguimiento realizado por el Área Seguridad de la Información AREIN del Grupo SISAM a la fecha no se ha registrado perdida, incidentes de activos de información acorde a los pilares del modelo de seguridad y privacidad de información.

17. BIBLIOGRAFÍA

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES (2018). Manual de Gobierno Digital. Bogotá

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES, Fortalecimiento de la Gestión TI en el Estado, https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

ISO/IEC/27001(2013). Sistema de Gestión de Seguridad de la Información. Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, Bogotá D.C.