DIRECCIÓN GENERAL
DE SANIDAD MILITAR

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2025

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 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 está construido de acuerdo con los parámetros de lenguaje claro emitidos por el Departamento Nacional de Planeación. 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”.
2	Noviembre 2022	Se actualiza de acuerdo con la información y nueva normativa. NOTA PROASIG - PROPLAES: 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 - 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. 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°

Versión	Fecha de Aprobación	Descripción de los cambios
		0124014880202 /MDN-COGFM-JEMCO-DIGSA-ARDEI-2.25, de fecha 30 de 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 - 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 Acta No. 0124014880202 de 30 de diciembre de 2024
Revisó:	TC. Jorge Darwin Guevara G. Coordinador Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA PD. Ángela María Tofiño Saavedra Coordinadora Grupo Asuntos Legales DIGSA PD. Alexandra Martínez Vargas Coordinadora Grupo de Planeación Estratégica DIGSA Representante de la Alta Dirección TASD. Yamile López Gestor de Calidad de Grupo Sistema Integral de Tecnologías de la Información y Comunicación DIGSA
Elaboró:	PD. Roberto Rodríguez Perdomo Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA Gestor Seguridad de la Información

Contenido

1. Presentación

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. FUNDAMENTO NORMATIVO

- 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 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.

- 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

5. 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.

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.

6. 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

7. 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:

7.1. 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.

7.2. 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.

8. 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.

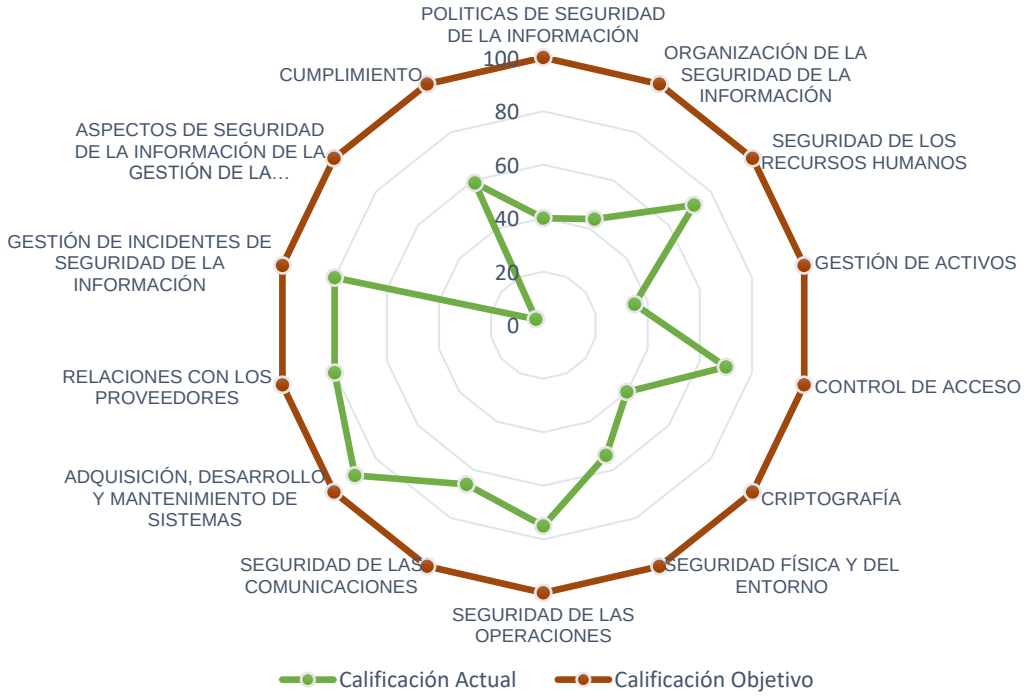
- Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

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.

9. AUTODIAGNOSTICO ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

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.

Grafica 1. Autodiagnóstico Estado Actual DIGSA



Fuente: 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/

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**
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**

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

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.

10. 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. Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

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.

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
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.
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: Elaboración propia

11. ACTIVIDADES A DESARROLLAR

Tabla 3. Cronograma de actividades a desarrollar

					Fecha Programada	
Ejes	Gestión	Actividades	Producto	Responsable	Fecha Inicial	Fecha Final
Control de Accesos	Implementar políticas de control de acceso	Autenticación del doble factor en los usuarios de la DIGSA	Informe número de funcionarios con implementación del doble factor de autenticación.	Área Seguridad de la Información-AREIN	05/03/2025	31/12/2025
Monitoreo de Redes y Sistemas	Realizar monitoreo en tiempo real de redes y sistemas	Detectar a través de un software actividades sospechosas	Informe de Mitigación vulnerabilidades y alertas de seguridad detectadas.	Área Seguridad de la Información-AREIN	05/03/2025	31/12/2025
Educación y Capacitación	Capacitar al personal de la DIGSA	Dictar charlas relacionadas con las buenas prácticas de ciberseguridad y concienciación sobre phishing y otras amenazas.	Capacitar al 100% del personal DIGSA en criterios de ciberseguridad,	Área Seguridad de la Información-AREIN	05/03/2025	31/12/2025

Fuente: Elaboración propia

12. 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
Servicio de renovación de garantía y soporte de los servidores con el fin de garantizar óptimas condiciones en la infraestructura tecnológica de la Dirección General de Sanidad Militar.	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 abarca la mejora continua de la infraestructura tecnológica en la Dirección General de Sanidad Militar. Al actualizar garantías y ofrecer soporte técnico especializado, se asegura el mantenimiento de los servidores, lo que se traduce en un rendimiento más estable y fiable. Este enfoque proactivo minimiza riesgos de fallos, prolonga la vida útil del equipo y garantiza una operación sin interrupciones. En consecuencia, la DIGSA experimentará una mayor eficiencia operativa, una mejor seguridad de los datos y una infraestructura tecnológica más robusta y resistente.	$ 63.320.000
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)	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	Mantener, dar soporte, actualizar y resolver problemas en los firewalls de la DIGSA y el Ministerio de Defensa Nacional (Edificio Fortaleza), así como en el XDR y el servicio de protección de correo electrónico FortiMail de la Dirección General de Sanidad Militar, impactará	$ 520.213.000,00

Proyecto	Objetivo	Alcance	Presupuesto
de la Dirección General de Sanidad Militar.	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 infraestructura tecnológica. Con estos servicios, la DIGSA logrará una mayor estabilidad operativa, reducirá vulnerabilidades y garantizará un entorno tecnológico más seguro y eficiente.	positivamente en la DIGSA al fortalecer la seguridad de la red y los sistemas. La gestión continua y la mejora de estas herramientas asegurarán una protección más robusta contra amenazas, garantizarán la integridad y confidencialidad de la información y permitirán un funcionamiento más seguro y eficiente de las infraestructuras tecnológicas 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	Adquirir y renovar licencias de Microsoft a través del acuerdo marco de precios y el instrumento de	Asegurar acceso continuo a versiones actualizadas y soporte técnico, optimizando el rendimiento de las aplicaciones y	$ 711.614.076,24

Proyecto	Objetivo	Alcance	Presupuesto
licenciamiento Microsoft mediante acuerdo marco de precios del instrumento de agregación de demanda software por catálogo para la Dirección General de Sanidad Militar.	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 desempeño general de la DIGSA.	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	

Fuente: Elaboración propia

13. 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.

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

Fuente: Elaboración propia

- 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.

14. SEGUIMIENTO

- **Indicador - Ejecución Plan de Seguridad de la Información**

Cumplimiento ejecución de las actividades propuestas.

Objetivo: Busca evaluar el nivel de eficacia en la ejecución de las actividades del Plan de Seguridad de la Información**.**

Tipo Indicador: Eficacia

- **Variables**

$$Eficacia\ PSPI = \frac{Numero\ de\ Actividades\ Ejecutadas}{Numero\ de\ Actividades\ Planeadas} * 100\% = \%\ Cumplimiento$$

Metas

Mínima	75 – 80 %	Satisfactoria	80 – 90 %	Sobresaliente	100%

- **Cumplimiento de Políticas de Seguridad de la Información**

Cumplimiento de políticas de seguridad de la información en la Dirección General de Sanidad Militar.

Objetivo: Busca identificar el nivel de estructuración de la Política de Seguridad de la Información.

Tipo Indicador: Cumplimiento

Variables

¿La Entidad ha definido una Política General de Seguridad de la Información?

Si se evidencia = 1 No se Evidencia = 0

¿La entidad ha definido una organización interna en términos de personas y responsabilidades con el fin de cumplir las políticas de seguridad de la información y documenta estas actividades?

Si se evidencia = 1 No se Evidencia = 0

Metas: Cumple = 1 No Cumple = 0

- **Indicador – Sensibilización Seguridad de la Información**

El indicador permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales. Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada por parte de los responsables de la capacitación y sensibilización.

Objetivo: El objetivo del indicador es establecer la efectividad de un plan de capacitación y sensibilización previamente definido como medio para el control de incidentes de seguridad.

Tipo Indicador: Gestión

Variables

$$Sensibilización\ SI = \frac{Numero\ de\ Personas\ Capacitadas}{Total\ de\ Personas\ a\ Capacitar} * 100\% = \%\ Cumplimiento$$

Metas

Mínima	75 – 80 %	Satisfactoria	80 – 90 %	Sobresaliente	100%

15. 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.

16. ANEXOS

Anexo 1: Grafica 1. Autodiagnóstico Estado Actual DIGSA
Anexo 2: Tabla 1. Evaluación de Efectividad de controles
Anexo 3: Tabla 2. Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones
Anexo 4: Tabla 3. Cronograma de actividades a desarrollar
Anexo 5: Tabla 4. Proyectos Contractuales
Anexo 6: Tabla 5. Esquemas de Líneas de Defensa de la DIGSA.