PLAN INSTITUCIONAL
DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

DIGSA 2023

SGSI
SISTEMA DE GESTION
DE SEGURIDAD DE LA INFORMACIÓN

CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de los cambios
1	Enero 2021	Versión Inicial. Elaboración por primera vez del documento. 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 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° 0120010254602, de fecha 16 de diciembre de 2020. 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.

CONTROL DE APROBACIÓN

Aprobó:	CR. Santiago Murillo Colmenares Subdirector Técnico y de Gestión DIGSA	
Revisó:	TADS. Yamile López Proceso Gestión Tecnologías de la Información y las Comunicaciones – PROGTIC - Gestor de Calidad	CR. José Mauricio Barrera Barrera Coordinador Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA (E)
	SMSM. Edna del Pilar Martínez Páez Grupo Planeación Estratégica DIGSA Líder Área Sistemas Integrados de Gestión ARSIG	PD. Alexandra Martínez Vargas Coordinadora Grupo Planeación Estratégica DIGSA Representante de la Alta Dirección
Elaboró:	OPS: Cristian Camilo Gantiva Rincon Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA Área Seguridad de la Información DIGSA	

Contenido

Tablas

Lista de Figuras

1. PRESENTACION

La política de Gobierno Digital es uno de los pilares del Estado en el proceso de transformación y modernización de las entidades públicas cuyo objetivo es promover la confianza en el entorno digital mediante el aprovechamiento de las tecnologías de la información y comunicaciones. Dentro de los elementos base que permiten el desarrollo de dicha política se encuentra el de Seguridad y Privacidad, el cual busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, con el fin de garantizar la continuidad de los sistemas de información, su buen uso y la privacidad de los datos, a través de un Modelo de Seguridad y Privacidad de la Información.

Debido a los múltiples riesgos y amenazas que en la actualidad atentan contra la seguridad de la información, la protección y la privacidad de los datos, se hace indispensable que la Dirección General de Sanidad Militar implemente, mantenga y optimice de manera continua un Sistema de Gestión de Seguridad de la Información.

Para realizar este modelo se requiere elaborar una serie de procesos, políticas y procedimientos que conllevan al cumplimiento de los lineamientos establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones. Por esta razón es necesario elaborar un Plan de Seguridad y Privacidad de la Información, con el fin de establecer las actividades que se deben realizar para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y de esta manera evaluar el nivel de madurez de la Dirección General de Sanidad Militar en la planificación, implementación y verificación del modelo.

Por lo anterior y teniendo en cuenta el resultado del análisis GAP realizado en la Dirección General de Sanidad Militar, con respecto a la norma NTC-ISO-IEC-207001:2013, el cual nos indica los riesgos en la seguridad de la Información a los que estamos expuestos y los controles que debemos implementar para la mitigación o eliminación de dichas amenazas, se puede evidenciar que la Dirección General de Sanidad Militar reconoce la importancia de la implementación de un Sistema de Gestión de Seguridad de la información SGSI y aunque existen un alcance, unos lineamientos y controles generales enfocados en la Seguridad de la Información; las políticas y procedimientos deben ser estandarizadas, formalizadas, codificadas, difundidas y disponibles para toda la Entidad.

Por otra parte, y en aras de incluir a nivel general a todos los funcionarios de la DIGSA en la importancia de la Seguridad de la Información, se han venido realizado una serie de campañas, capacitaciones y tips difundidos a los empleados, con el fin de crear conciencia entre los funcionarios de la Dirección frente a las políticas de Seguridad de la Información y sus buenas prácticas.

2. POLITICA DE SEGURIDAD DE LA INFORMACION DIGSA

La Dirección General de Sanidad Militar, como entidad encargada de asegurar la prestación de los servicios de salud del personal afiliado y beneficiario del Subsistema de Salud de las Fuerzas Militares, reconoce la importancia de identificar y proteger sus activos de información frente a riesgos asociados, así como propender por los principios de seguridad de la información, relacionados con su confidencialidad, disponibilidad e integridad; comprometiéndose a establecer, implementar, mantener, evaluar, gestionar, proteger, preservar y mejorar continuamente su Sistema de Gestión de Seguridad de la Información – SGSI, bajo los aspectos del ordenamiento legal, sus objetivos estratégicos y código de integridad.

3. OBJETIVOS DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION

3.1 Objetivo General

Establecer las actividades que se planean realizar para implementar el Sistema de Gestión de Seguridad de la Información de la DIGSA, mediante la adopción del modelo de Seguridad y Privacidad de la Información con la finalidad de fortalecer el aseguramiento de los servicios de TI y preservar la confidencialidad, integridad, disponibilidad y privacidad de los activos de información de la Dirección General de Sanidad Militar, así como la de sus partes interesadas.

3.2 Objetivos Específicos

- Incrementar el nivel de madurez de la DIGSA frente a la gestión de seguridad y privacidad de la información.
- Preservar la confidencialidad, integridad y disponibilidad de la información, de acuerdo a las políticas, procesos y procedimientos desarrollados, para la gestión del SGSI.
- Gestionar de forma concreta, adecuada y permanente los riesgos de seguridad de la información a los que puedan estar los activos de información de la entidad dentro del alcance del SGSI en DIGSA.
- Fortalecer la cultura con respecto a seguridad de la información a los funcionarios de la DIGSA, usuarios externos, terceros y demás partes interesadas de la entidad.
- Cumplir con los requisitos legales y normativos en materia de Seguridad y privacidad, seguridad digital y protección de la información personal.

4. ALCANCE

Se definirán las actividades a cumplir durante la presente vigencia (2023) para avanzar en la implementación del Sistema de Gestión de Seguridad de la Información de la Dirección General de Sanidad Militar, aplica a los activos de información de las diferentes áreas que la conforman y que manejan los procesos misionales y el proceso de apoyo relacionado con la Gestión de Tecnología, conforme a lo establecido en el mapa de procesos y es de obligatorio cumplimiento por parte de todos los funcionarios, contratistas y terceras partes que presten sus servicios a la Dirección General de Sanidad Militar.

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

5. FUNDAMENTO NORMATIVO

- Ley 527 del 18 agosto de 1999 “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.

- Ley 1273 del 5 enero de 2009 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

- Ley 1341 del 30 julio del 2009. “Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto número 1078 del 26 mayo de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 del 18 enero de 2011 y el artículo 45 de la Ley 1753 del 09 julio de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales

- Ley 1581 del 17 octubre de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.

- Ley 1712 del 06 marzo de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”. Decisión Andina 351 de 2015 “Régimen común sobre derecho de autor y derechos conexos”.

- Decreto 1377 del 27 junio de 2013. “Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.

- Decreto 2573 del 12 diciembre de 2014 “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea…”, donde se encuentra como componente el Modelo de Seguridad y Privacidad de la Información.

- Decreto 1078 del 26 mayo de 2015 modificado por el Decreto 1008 de 14 junio de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.

- Decreto 1413 del 25 agosto de 2017 “Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto número 1078 del 26 mayo de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 del 18 enero de 2011 y el artículo 45 de la Ley 1753 del 09 junio de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

- Decreto 1499 del 11 septiembre de 2017, el cual modificó el Decreto 1083 del 26 mayo de 2015 – Modelo Integrado de Planeación y Gestión.

- Directiva Permanente Nro. DIR2014-18 “Políticas de Seguridad de la Información para el Sector Defensa”.

- CONPES 3854 del 07 marzo de 2017 – Política de Seguridad Digital del Estado Colombiano.

- Directiva Permanente No. 154 /MDN-CGFM-JEMC-SEMCO-JEIMC-DIRCO-23.1 “Políticas de Seguridad de las Información para las Fuerzas Militares”.

- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital año 2018.

- Norma Técnica Colombiana ISO27001:2013. Sistemas de Gestión de Seguridad de la Información

- Norma Técnica Colombiana ISO31000:2013. Gestión del Riesgo Principios y Directrices.

6. DEFINICIONES

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

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

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

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

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

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

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

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

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

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

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

Política: Declaración de alto nivel que describe la posición de la organización sobre un desempeño especifico.

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

Plan de tratamiento de riesgos MDN-COGFM-PROGTIC-DIGSA-PL-1: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

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

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

Responsable del tratamiento: Persona natural o jurídica, pública o privada. Que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

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

Rol: papel, función que alguien o algo desempeña.

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

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

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

Seguridad digital: preservación de los tres pilares fundamentales de la seguridad informática (integridad, confidencialidad y disponibilidad) que se encuentran en medios digitales.

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

7. ACRONIMOS

DIGSA: Dirección General de Sanidad Militar.

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

8. CONTEXTO

El presente plan está alineado y contribuye al logro de la misión, visión y demás elementos del direccionamiento estratégico de la Dirección General de Sanidad Militar.

ARTICULACION CON EL CONTEXTO ESTRATEGICO			
OBJETIVO ESTRATEGICO AL QUE APORTA	Fortalecer el desarrollo, implementación e integración del sistema de información en los procesos de aseguramiento y la prestación de los servicios de salud	Tecnologías de la Información y comunicaciones	Sistema de Gestión de Seguridad de la información
GESTION Y DESEMPEÑO INSTITUCIONAL MIPG	Política de Gobierno Digital Política de Seguridad Digital		

Tabla 1. Articulación con el contexto estratégico

9. ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACION

La estructura de seguridad de la información en la Dirección General de Sanidad Militar y teniendo en cuenta el MSPI (Modelo de Seguridad y Privacidad de la Información) en el cual debe estar representado por miembros, directivos y representantes de las áreas misionales garantizando que sea un proceso transversal uno dependa exclusivamente del área de TI estará conformada por los siguientes actores o roles[1].

9.1 Comité Institucional de Gestión y Desempeño

Responsable de revisar y aprobar la implementación y operación del Sistema de Gestión de Seguridad de la Información SGSI.

[1] Norma Internacional ISO 27001(2013). A.6.1.1. Sistema de Gestión de Seguridad de la Información. Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC. Bogotá D.C., 2013

9.2 Grupos Internos de Trabajo

- Grupo Sistema Integral de Información- Tecnologías de la Información y las Comunicaciones- Área Seguridad de la Información

  Responsable de presentar ante el Comité Institucional de Gestión y Desempeño la documentación, estrategias, propuestas, medidas y acciones a que haya lugar, para la implementación y el mantenimiento del SGSI, con el fin de garantizar la confiabilidad, disponibilidad e integridad de la seguridad de la información y promover la difusión y sensibilización al interior de la DIGSA en temas de seguridad de la información.

- Grupo Sistema Integral de Información- Tecnologías de la Información y las Comunicaciones- Área Infraestructura Redes y Comunicaciones- Área Administración del Sistema y Bases de Datos

  Responsables de seguir con los lineamientos establecidos en las políticas, procesos y procedimientos de seguridad de la información, implementando las medidas técnicas y los controles de seguridad informática en los recursos de tecnologías de la información y las comunicaciones, para brindar un nivel apropiado de seguridad de la información.

- Grupo de Planeación Estratégica

  Encargado revisar y controlar los documentos (políticas, procedimientos, manuales, guías, estándares, entre otros.) que se agreguen del Sistema de Gestión de Seguridad de la Información.

- Grupo de Talento Humano

  Encargado de comunicar los derechos y establecer las responsabilidades legales que adquiere cada funcionario, contratista o tercero, con relación al manejo y protección de los datos institucionales al interior de la DIGSA como fuera de las instalaciones.

  Así mismo es responsable de Incluir en los contratos cláusulas de confidencialidad y no divulgación de la información, así como la obligatoriedad en el cumplimiento de las políticas de seguridad de la información de la Dirección General de Sanidad Militar. Lo anterior a través del documento de confidencialidad denominado “Acta de Compromiso de Reserva, Seguridad y Calidad de la Información Personal Militar – Civil Planta y Civil Vinculado por Contrato o Convenio”, el cual deberá ser parte integral de los contratos.

  Debe informar al Grupo Sistema Integral de Información- Tecnologías de la Información y las Comunicaciones, las novedades de los funcionarios de planta y/o prestación de servicios (nombramiento, retiro, vacaciones, licencias, cambio de cargo, incapacidades, otros), con el fin de crear, modificar o cancelar las cuentas en el directorio activo y por ende los permisos de acceso a las aplicaciones y plataformas tecnológicas de la DIGSA.

Liderar los programas de inducción, reinducción, capacitación y sensibilización enfocados a fortalecer la toma de conciencia en relación con seguridad de la información.

- Grupo Contratación

  Encargado de incorporar las cláusulas en materia de seguridad de la información en los contratos, acuerdos u otra documentación que la entidad firme con contratistas y/o terceros. Por medio de los documentos denominados “Acta Compromiso de Reserva Externos” y “Acuerdo de Confidencialidad Sector Defensa – Anexo C”, los cuales deberán reflejarse en los respectivos contratos.

- Grupo Apoyo Administrativo

  Encargado de gestionar la seguridad y accesos físicos en cada una de las Áreas de la DIGSA, realizando las respectivas coordinaciones con el edificio y demás dependencias que requieran el acceso de terceros y/o retirar elementos que contengan cualquier tipo de información relevante para la DIGSA, dejando la respectiva trazabilidad.

- Grupo Asuntos Legales

  Encargado de brindar asesoría legal a la DIGSA, en lo que refiere al cumplimiento a las disposiciones normativas constitucionales y legales relacionada con la seguridad de la información, protección de datos personales, y transparencia al acceso a la información pública, para garantizar una adecuada toma de decisiones y mantener la unidad de criterio en la aplicación de dichas disposiciones.

- Área Seguimiento y Evaluación Institucional

  Responsable de realizar la evaluación y seguimiento al cumplimiento de las políticas, lineamientos y requisitos de Seguridad de la Información, así como auditar el SGSI.

- Subdirecciones, Grupos y Áreas de la DIGSA

  Todos los funcionarios de la DIGSA deberán aplicar y cumplir con las políticas, lineamientos, procesos, procedimientos de Seguridad de la Información, brindar un uso apropiado a los activos de información y asistir a las capacitaciones y/o sensibilizaciones que se realicen al interior de la DIGSA en temas de seguridad de la información.

10. DESARROLLO DEL PLAN DE SEGURIDAD DE LA INFORMACION

La metodología de implementación del Plan de Seguridad y Privacidad para la Dirección General de Sanidad Militar-DIGSA, está basado en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) y lo establecido en el Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, que contempla un ciclo de operación que consta de

cinco (5) fases, las cuales permiten que la DIGSA pueda gestionar adecuadamente la seguridad y privacidad de sus activos de información, así:

Figura 1 Ciclo de Operación del Modelo de Seguridad de la Información

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

10.1 Fase de Diagnostico Seguridad de la Información

- Se identificó el estado actual de madurez de la DIGSA con la actualización de los activos de información en las áreas que la conforman, respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

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

10.2 Fase de Planificación

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

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

- Se revisó el Manual de Políticas de Seguridad y Privacidad de la Información con el fin de identificar procesos a actualizar.

- Se elaboraron los procedimientos de seguridad de la información.

- Se elaboró la matriz GAP para la identificación, criticidad, nivel de impacto, Identificación de las Infraestructuras Críticas Cibernéticas (ICC) y la clasificación de la información de los activos de información de la Dirección General de Sanidad Militar – DIGSA.

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

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

10.3 Fase de Implementación

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

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

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

10.4 Actividades de Seguridad y Privacidad de la Información vigencia 2023

Para la vigencia 2023 se realizarán las siguientes actividades para continuar con la implementación del Sistema de Gestión de Seguridad de la información, las cuales se encuentran enmarcadas en el objetivo No.3 del plan de acción del Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, así:

No.	Actividad	Objetivos	Evidencia actividad	Fecha	Indicador
1.	evaluar el nivel de madurez de Seguridad y Privacidad de la Información en la DIGSA	Determinar el estado de avance de la gestión de seguridad y privacidad de la información y actualizar su alcance.	Diligenciamiento de la herramienta de diagnóstico.	Enero-Marzo	15%

2.	Realizar seguimiento al Modelo de Seguridad y Privacidad de la Información a través del diligenciamiento del FURAG-Política de Seguridad Digital.	Dar cumplimiento a lo establecido por la Política de Seguridad Digital (FURAG)	Diligenciamiento formulario FURAG correspondiente a la Política de Seguridad Digital	Enero-Junio	10%
3.	Realizar sensibilización y comunicación en seguridad y privacidad de la información.	Generar cultura de seguridad y privacidad de la información al interior de la DIGSA.	Actualizar el plan de Sensibilización, Comunicación y capacitación referente a seguridad de la información, dirigido a todos los funcionarios de la DIGSA.	Enero-Junio	15%
			Boletines de Seguridad de la Información. Tips de seguridad de la información enviadas de manera masiva por correo electrónico. Actas de Asistencia a charlas de seguridad.	Enero-Diciembre	25%
4.	Coordinar con el CCOCI, las pruebas de seguridad, el monitoreo, análisis y gestión de incidentes de	Gestionar de forma oportuna y eficiente los informes emitidos por el CCOCI, para evitar afectaciones	Informes y alertas de análisis de vulnerabilidades e incidentes cibernéticos reportados por el CCOCI.	Trimestral	25%

	los servicios de Seguridad de la Información.	en los sistemas informáticos.			
5.	Implementar y gestionar los controles establecidos en la Declaración de Aplicabilidad	Verificar el cumplimiento de los controles establecidos en la declaración de aplicabilidad de la DIGSA.	Informe de verificación la Matriz de Aplicabilidad	Junio-Diciembre	20%
6.	Acompañar al Grupo de Planeación Estratégica en el seguimiento a la implementación de los planes de tratamiento de riesgos de seguridad digital que adopten los procesos	Verificar el cumplimento de los planes de riesgos de la seguridad digital.	Informe de seguimiento del análisis, evaluación y tratamiento de riesgos de los activos de información que fueron catalogados con nivel de criticidad alto en cada uno de los procesos de la DIGSA durante la vigencia 2023.	Marzo-Junio	25%

Tabla 2. Actividades de Seguridad y Privacidad de la Información

11. INDICADOR

PORCENTAJE DE CONTENIDO BLOQUEADO.
Este indicador permite controlar los incidentes de seguridad informática y prevenir los posibles incidentes a través de la red y a los servidores.

12. META

Se espera que el porcentaje de Contenido Bloqueado no supere el 5% del total de incidentes resueltos

13. POLITICAS DE OPERACION

- Cumplir con las disposiciones normativas vigentes aplicables al Sistema de Gestión de Seguridad de la Información.
- Validar y monitorear, de manera periódica, la implementación de los controles de seguridad establecidos.
- Todos los usuarios deben mantener reserva absoluta con respecto a la información de la DIGSA o de sus funcionarios que manejen información relevante o de importancia debido a sus funciones.
- Comunicar los derechos y establecer las responsabilidades legales que adquiere cada funcionario, contratista o tercero, con relación al manejo y protección de los datos institucionales tanto al interior como fuera de las instalaciones.
- Realizar la clasificación de la información, evaluando las tres características de la información en las cuales de basa la seguridad de la información: confidencialidad, integridad y disponibilidad.

14. SOCIALIZACION

- Publicación en la página web de la Dirección General de Sanidad Militar https://www.sanidadfuerzasmilitares.mil.co en Inicio\Transparencia y Acceso a la Información Pública\ 4. Planeación, Presupuesto e Informes\ 4.11 Planes Institucionales
- Cargue del plan institucional de Seguridad y Privacidad de la Información PSPI DIGSA en la SuiteVision (SVE)
- Sensibilización semestral a los funcionarios DIGSA
- Plan de Sensibilización y Comunicación Seguridad de la Información DIGSA. MDN-COGFM-PROGTIC-DIGSA-PL-3

15. SEGUIMIENTO AL PLAN INSTITUCIONAL

Seguimiento a las actividades del plan de acción programadas 2023 cumpliendo con el OBJ. 3. Fortalecer el Desarrollo, Implementación e Integración del Sistema de Información en los procesos de aseguramiento y la Prestación de los Servicios de Salud Tecnologías de la información y comunicaciones a realizar durante el año.

16. BIBLIOGRAFIA

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.