DIRECCIÓN GENERAL
DE SANIDAD MILITAR

Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información

2025

CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de los cambios
1	Octubre 2020	Versión Inicial. Elaboración por primera vez del documento.
2	Enero 2021	Este Plan fue aprobado en sesión de Comité de Gestión y Desempeño Institucional, documentado mediante Acta N° 0120010254602, de fecha 16 de diciembre de 2020.
3	Enero 2022	Se actualizaron las actividades a desarrollar durante el año 2022. Este Plan fue aprobado en sesión de Comité de Gestión y Desempeño Institucional, documentado mediante Acta N° 0121013721902, de fecha 27 de diciembre de 2021.
4	Noviembre 2022	Se actualiza de acuerdo con la información y 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, SanidadNaval, Jefatura Salud de la Fuerza Aérea y los Coordinadores de Grupode 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 delproceso que lo emite. Fue traducido a lenguaje claro.
5	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 No 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 Guerrero Coordinador Grupo Sistema Integral de Tecnologías de la Información y Comunicación 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 Gestor Seguridad de la Información del Grupo Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones DIGSA

Contenido

LISTA TABLAS

LISTA ILUSTRACIONES

1. Presentación

La política de seguridad de la información de la Dirección General de Sanidad Militar tiene como objetivo la protección de los activos de información ante una serie de amenazas o brechas que atenten contra los principios fundamentales de la seguridad, como lo son la perdida de la confidencialidad, integridad y Disponibilidad que posiblemente puedan afectar la continuidad de la DIGSA. Por ello mediante la definición del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se busca identificar las amenazas, las vulnerabilidades, el impacto y el nivel de riesgos asociados a los activos de información, así como el tratamiento, evaluación y monitoreo de los mismos.

Teniendo como referencia el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y el Sistema de Gestión de Seguridad de la Información –SGSI que se encuentra en proceso de implementación en la Dirección General de Sanidad Militar y basados en un enfoque de planeación de gestión del riesgo, se busca prevenir los efectos no deseados que puedan presentarse en cuanto a seguridad de la información; por lo cual es importante establecer y controlar la gestión de incidentes que afecten los activos de información e implantar unas contramedidas para disminuir la probabilidad de su materialización.

Lo anterior se realiza en cumplimiento a la normatividad establecida por el estado colombiano, a través del CONPES 3854 del 07 enero de 2017, el Modelo de Seguridad y Privacidad de MINTIC, el Decreto 1008 de 14 de junio 2018 y adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública.

2. Objetivo General

Con el objetivo de salvaguardar la integridad, confidencialidad y disponibilidad de la información, así como de garantizar la seguridad digital y continuidad operacional de los servicios, se establecerán lineamientos que permitan realizar un análisis exhaustivo de los riesgos a los que se encuentra expuesta la Dirección General de Sanidad Militar. Estas medidas permitirán evaluar y tratar de manera proactiva cualquier amenaza potencial, asegurando así la protección de los activos de información de la institución.

3. Alcance

Con el fin de proteger la integridad, confidencialidad, disponibilidad y autenticidad de la información, se capacitará a los funcionarios de la Dirección General de Sanidad Militar en la identificación y gestión de riesgos de seguridad de la información. Esta capacitación se basará en los lineamientos del DAFP y la norma ISO 31000:2018. Es importante destacar que todas las Direcciones de Sanidad deberán cumplir con esta política, independientemente de la dependencia en la cual estén abordo laborando. Se implementarán programas de capacitación virtualmente en gestión de riesgos de seguridad de la información alineado con los estándares DAFP e ISO 31000:2018 en la cual se verificará la asistencia de todo el personal que conforma la Dirección General de Sanidad Militar y sus dependencias, con el fin de garantizar la protección de los activos de información.

4. Fundamento Normativo

Tabla 1. Fundamento Normativo

NORMA	OBJETIVO
Ley 527 del 21 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

NORMA	OBJETIVO
Ley 1273 del 05 de 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 de 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 junio 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
Decreto 1377 del 27 junio de 2013	Por el cual se reglamenta parcialmente la Ley 1581 del 17 octubre 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	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1008 del junio 14 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 del 26 mayo de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Resolución 0463 del 9 de febrero del 2022	Por medio del cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones
Resolución 7870 del 26 de diciembre del 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
Directiva Permanente No. 154 /MDN-CGFM- JEMC-SEMCO-JEIMC- DIRCO-23.1 del 19 junio de 2014	Políticas de Seguridad de las Información para las Fuerzas Militares.
CONPES 3854 del 07 marzo de 2017	Política de Seguridad Digital del Estado Colombiano
Dirección de Gestión y Desempeño Institucional, noviembre 2022 – DAFP	Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6.
DIGSA octubre del 2021	Guía para la Administración del Riesgo SSFM DIGSA MDN- COGFM-PROPLAES-DIGSA-GI.95.1-2

NORMA	OBJETIVO
Norma Técnica Colombiana ISO27001:2013	Sistemas de Gestión de Seguridad de la Información.
Norma Técnica Colombiana ISO31000:2013	Gestión del Riesgo Principios y Directrices
Decreto 612 de 2018	Directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado

Fuente: Elaboración propia SISAM

5. Definiciones

Acción: Proceso de realización de algo que implica cambio o movimiento. Se determina mediante verbos que indican la acción que deben realizar como parte del control.

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

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.

Compartir o transferir el riesgo: Opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como seguros o sitios alternos.

Consecuencia: Efectos que se pueden presentar cuando un riesgo se materializa.

Control: Medida que permite reducir o mitigar el riesgo determinado por el proceso (políticas, dispositivos, prácticas u otras acciones).

Evaluación del riesgo: Resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo

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.

Identificación del riesgo: Etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgos definidos.

Impacto: Son las consecuencias que genera un riesgo una vez se materialice.

Mapa de Riesgos: Documento que consolida la información resultante en cada una de las etapas de la Gestión del riesgo

Materialización del riesgo: Ocurrencia del riesgo identificado

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.

Probabilidad: Es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

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: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Riesgo inherente: Nivel del riesgo propio de la actividad, es aquel al que se enfrenta la entidad en ausencia de acciones para modificar su probabilidad o impacto

Riesgo residual: Nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.

Tolerancia al riesgo: Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes.
Valoración del riesgo: Establece la identificación y evaluación de los controles, para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización.

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

6. Acrónimos

ARECO:	Área de Infraestructura Tecnológica, Redes y Comunicaciones
AREIN:	Área de Seguridad de la Información
ARIBD:	Área administración del Sistema y Base de Datos
CCOC:	Comando Conjunto Cibernético del Comando General de las Fuerzas Militares de Colombia
DIGSA:	Dirección General de Sanidad Militar
GRSD:	Gestión de Riesgos de Seguridad Digital
GRSD:	Gestión de Riesgos de Seguridad Digita
ICC:	Infraestructura Critica Cibernética
MGRSD:	Modelo Nacional de Gestión de Riesgos de Seguridad Digital
MINTIC:	Ministerio de Tecnologías de la Información y las Comunicaciones
MSPI:	Modelo de Seguridad y Privacidad de la Información.
PIC:	Plan Institucional de Capacitaciones
SGSI:	Sistema de Gestión de Seguridad de la Información.
SISAM:	Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones

7. Política

La DIGSA clasificará su información según confidencialidad, integridad y disponibilidad, utilizando la Matriz de Activos de Información MDN-COGFM-PROGTIC-DIGSA-MT.95.1-1. El objetivo es proteger los activos de información, minimizando el impacto de los riesgos identificados y asegurando la continuidad de los servicios. Se implementarán controles técnicos y administrativos para cumplir con las normas vigentes y las políticas de seguridad de la información, incluyendo la política de riesgos integrada. Esto garantizará la protección de la información, incluso en equipos que son retirados de las instalaciones. Además, se deshabilitarán los recursos innecesarios para evitar riesgos innecesarios. Estableciendo estos controles de

seguridad alineados con la política de riesgos se integra para garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los activos de información, incluyendo aquellos que son retirados de las instalaciones.

- Realizar la clasificación de la información, evaluando las tres características de la información en las cuales se basa la seguridad de la información: confidencialidad, integridad y disponibilidad en Matriz de Activos de Información DIGSA MDN-COGFM-PROGTIC-DIGSA-MT.95.1-1.

- Para la DIGSA, la protección de la información busca la disminución del impacto generado sobre los activos de información por los riesgos identificados de manera sistemática; con el propósito de mantener un nivel aceptable de exposición que permita responder por la confidencialidad, disponibilidad e integridad de la información, acorde con las necesidades de los diferentes grupos de interés identificados.

- Los equipos de cómputo o activos de información que por razones del servicio se retiren de las instalaciones de la DIGSA, deberán contener únicamente la información estrictamente necesaria para el cumplimiento de su misión y se deshabilitarán los recursos que no se requieran o que puedan poner en riesgo la información que contiene.

- Cumplir con las disposiciones normativas vigentes aplicables al Sistema de Gestión de Seguridad de la Información.

- Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de Seguridad de la Información.

- Definir claramente las funciones y tareas que desempeñará el funcionario en el cargo con el fin de establecer la responsabilidad en el manejo de la información, teniendo en cuenta la clasificación de esta y el cumplimiento de las políticas de seguridad de la información.

8. Metodología

La DIGSA ha adoptado una metodología de gestión de riesgos de seguridad de la información alineada con las mejores prácticas nacionales e internacionales, como las guías del DAFP y el MINTIC. Este enfoque, adaptado al contexto específico de la entidad, incluye un plan de riesgos detallado que define las actividades para identificar, evaluar, tratar y monitorear los riesgos. A través de este plan, la DIGSA garantiza la protección de sus activos de información y la continuidad de sus operaciones.

Relacionando en la siguiente tabla los 05 riesgos, cada uno con sus respectivos controles a lo cual se le realiza un seguimiento trimestral, evidenciando esta actividad en un informe detallado con evidencias y cargadola en la plataforma Suiteve Visión Empresarial.

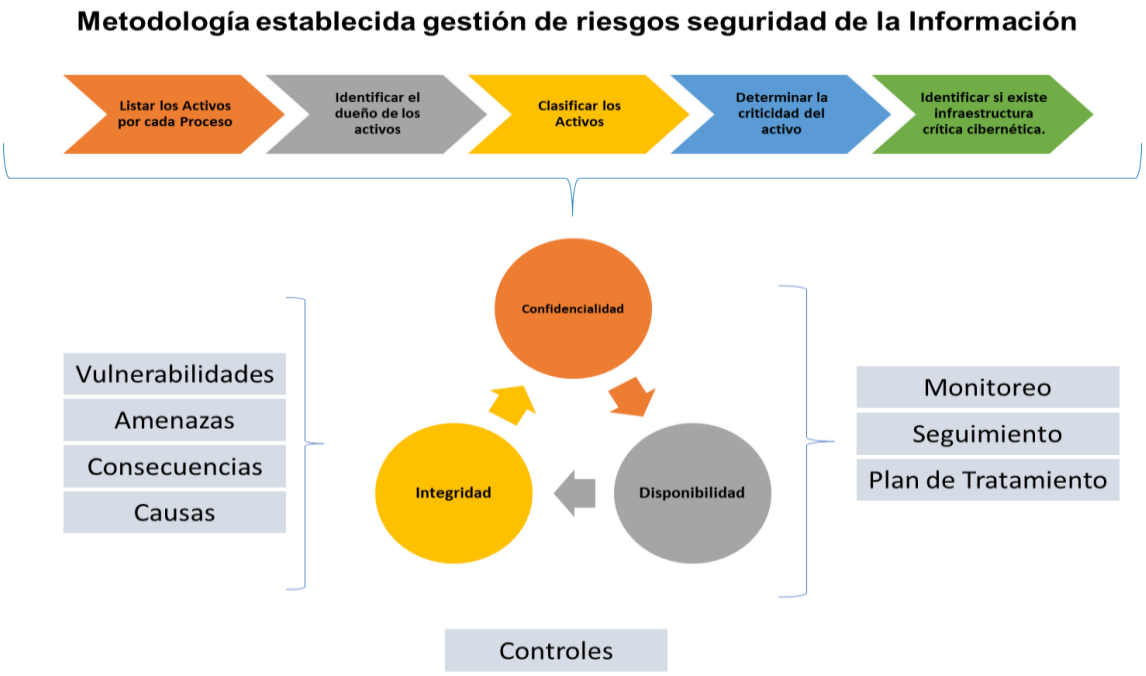
Tabla 2. Relación de los Riesgos y Controles SISAM – DIGSA

ítem	Nombre de los Riegos	Controles del Riesgo	Nivel del Riesgo	Seguimiento y Monitoreo	Actividad	Responsable	Fecha Cumplimiento
1	Posibilidad de Afectación Económica y Reputacional por pérdida de la integridad y disponibilidad de la información debido a fallas en la infraestructura tecnológica, de comunicaciones y sistemas de información. - PROGTIC – SISAM.	• Gestión de las vulnerabilidades técnicas • Controles de redes • Seguridad de los servicios de red • Políticas y procedimientos de transferencia de información • Cadena de suministro de tecnología de información y comunicación	Alto	Trimestral	Informe trimestral cargándolo en la Suiteve Visión	Área Seguridad de la Información y Gestor de Calidad SISAM	Trimestralmente
2	Posibilidad de Afectación Económica y Reputacional por perdida de la integridad confidencialidad de la información debido eliminación de información reservada o Publica pérdida, hurto, fuga, destrucción y/o desviación de información, por accesos no autorizados de usuarios debido a la inadecuada gestión de permisos de acceso a los sistemas de información.	• Política de control de acceso. • Política sobre el uso de los servicios de red. • Cancelación del registro de usuarios. • Suministro de acceso de usuarios. • Gestión de información de autenticación secreta de usuarios. • Retiro o ajuste de los derechos de acceso. • Acuerdos de confidencialidad o de no divulgación.	Alto	Trimestral	Informe trimestral cargándolo en la Suiteve Visión	Área Seguridad de la Información y Gestor de Calidad SISAM	Trimestralmente
3	Posibilidad de Afectación Económica y Reputacional por pérdida de la integridad, disponibilidad y confidencialidad de la información por la eliminación, hurto o fuga de información pública o reservada debido a ataques cibernéticos.	• Controles contra códigos maliciosos. • Teletrabajo. • Política sobre el uso de controles criptográficos. • Seguridad del cableado. • Seguridad de equipos y activos fuera de las instalaciones. • Protección de registros.	Alto	Trimestral	Informe trimestral cargándolo en la Suit Visión	Área Seguridad de la Información y Gestor de Calidad SISAM	Trimestralmente
4	Posibilidad de Afectación Económica y Reputacional por pérdida de la integridad, disponibilidad de la información por pérdida de activos de información debido a desastres o eventos fortuitos.	• Respaldo de información. • Gestión de las vulnerabilidades técnicas.	Alto	Trimestral	Informe trimestral cargándolo en la Suit Visión	Área Seguridad de la Información y Gestor de Calidad SISAM	Trimestralmente
5	Posibilidad de Afectación Económica y Reputacional por perdida de la disponibilidad de la información por uso y administración no autorizada de servidores y equipos de comunicación debido a la	• Perímetro de seguridad física. • Controles físicos de entrada. • Política de control de acceso. • Sistema de gestión de contraseñas. • Ubicación y	Alto	Trimestral	Informe trimestral cargándolo en la Suit Visión	Área Seguridad de la Información y Gestor de Calidad SISAM	Trimestralmente

ítem	Nombre de los Riegos	Controles del Riesgo	Nivel del Riesgo	Seguimiento y Monitoreo	Actividad	Responsable	Fecha Cumplimiento
	inadecuada gestión de roles para la administración y gestión de la infraestructura tecnológica.	protección de los equipos. • Registros del administrador y del operador.					

Fuente: Elaboración propia SISAM

Ilustración 1. Metodología Identificación Riesgos Seguridad de la Información



Fuente: Elaboración propia SISAM

8.1. Identificación del Riesgo

Teniendo en cuenta la anterior gráfica, el primer paso para la identificación de riesgos es necesario la identificación de los activos de información, los cuales acorde a los lineamientos establecidos deberán ser clasificados dentro del marco normativo de la ley 1712 de 2014, Ley 1581 de 2012 y los tres tipos de riesgos inherentes de seguridad de la información como son la Confidencialidad, Integridad, Disponibilidad, todo lo anterior asociado las diferentes amenazas y vulnerabilidades, que a su vez estará asociado a las causas y consecuencias que genere una posible materialización (Anexo 4 técnico Modelo Nacional de Gestión de Riesgos de Seguridad de la Información en Entidades Públicas). La siguiente grafica muestra la metodología establecida dentro de la gestión de riesgos.

8.2. Criterios de Evaluación de Riesgos de Seguridad de la Información

La evaluación de los riesgos de seguridad de la información se enfocará en:

- El valor estratégico del proceso de información en la DIGSA
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios.

- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de la DIGSA.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la DIGSA.

8.3. Criterios de Impacto

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la DIGSA, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceras partes)
- Pérdida del negocio y del valor financiero
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

8.4. Valoración de los Riesgos de Seguridad de la Información

Previo a la valoración de riesgos de seguridad de la información se determina la relevancia de identificar un inventario de activos de información de los procesos, el cual será la base del enfoque de la valoración de los riesgos de seguridad de la información. Se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la DIGSA, en esta fase se realizan las siguientes actividades:

- Análisis del riesgo: Se realiza la identificación de los riesgos y la estimación del riesgo.
- Evaluación del riesgo: La evaluación del riesgo requiere de una evaluación de los controles existentes.

8.5. Tratamiento de Riesgos de Seguridad de la Información

Está claro que no todos los riesgos tienen el mismo nivel de criticidad y que su gestión implica una serie de esfuerzos y costos en los que debe incurrir la entidad, de ahí la importancia que los líderes de proceso evalúen las opciones existentes en materia de tratamiento del riesgo para la mitigación del riesgo, así como la relación costo-beneficio de las medidas de tratamiento, dicha decisión puede ser:

Reducir: Adopta medidas para reducir la probabilidad o impacto, esto se determina mediante transferencia o mitigación.
Aceptar: No se adopta ninguna medida, se asume el mismo conociendo los efectos al materializarse.
Evitar: Busca minimizar la probabilidad de materialización del riesgo.
Mitigar: Implementar acciones que mitiguen el nivel del riesgo, pueden estar asociadas al plan de acción.
Transferir: Reduce la probabilidad o el impacto, la mejor estrategia es tercerizar el proceso o trasladarlo a través de pólizas o seguros.

8.6. Monitoreo y seguimiento de los Riesgos de Seguridad de la Información

En alineación con la dimensión 7 “Control interno” del Modelo Integrado de Planeación y Gestión – MIPG, se establece la responsabilidad y control, para la gestión del riesgo la cual es desarrollada por los funcionarios de la entidad., Nuevas amenazas, Cambios o aparición de nuevas vulnerabilidades, Aumento de las consecuencias o impactos, Incidentes de seguridad de la información.

8.7. Monitoreo y Seguimiento

La Dirección General de Sanidad Militar - DIGSA debe asegurar el logro de los objetivos, interesándose por el monitoreo y seguimiento periódico de los riesgos de la entidad (impactos, amenazas, vulnerabilidades y probabilidades), en busca de posibles cambios que requieran la valoración; esta acción debe ser realizada por el responsable o gestor del riesgo, anexando sus debidas evidencias de acuerdo con lo establecido en los controles. Desde el Grupo de Sistema Integral de Información Tecnologías de la Información y las Comunicaciones, se realizará seguimiento mensual con consolidación trimestral acorde a la Guía de Administración de Riesgos DIGSA, igualmente a través de las Tres Líneas de Defensa definidas en el Modelo Integrado de Planeación y Gestión - MIPG, en su Dimensión 7 Control Interno, a continuación, se presentan los roles dentro de Esquema de líneas de defensa del Sistema de Control Interno:

Tabla 3. Roles Esquema Línea de Defensa SCI

LÍNEAS DE DEFENSA	ROL PRINCIPAL	ACTIVIDADES EN EL SISTEMA DE CONTROL INTERNO (SCI)
Línea Estratégica Instancia decisoria dentro del Sistema de Control Interno, cuya responsabilidad recae en la Alta Dirección el Comité Institucional de Gestión y Desempeño y el Subcomité de Evaluación y Desempeño.	Analizar riesgos y amenazas que afectan el cumplimiento de los Planes Institucionales y Estratégicos, igualmente definir los lineamientos para la gestión del riesgo.	• Evaluación de la Política de riesgos • Monitoreo al estado de los riesgos aceptados (apetito por el riesgo), con el fin de identificar cambios sustantivos que afecten el funcionamiento de la entidad.
Primera Línea de Defensa Responsables Lideres y Coordinadores de Grupo, Equipos de Trabajo (en general servidores públicos y contratistas de todos los niveles de la Dirección General de Sanidad Militar).	Realizar el mantenimiento efectivo de controles, implementación de la metodología, ejecución de la política, y procedimientos de riesgos, su responsabilidad como primera línea es la identificación, evaluación, control y mitigación de los riesgos a través del Autocontrol.	• Verificación de la adecuada identificación de los riesgos. • Revisión de las exposiciones al riesgo con los grupos de valor, proveedores, sectores económicos u otros (monitoreo del contexto estratégico). • Generación de reportes periódicamente al Subcomité Seguimiento y Evaluación del cumplimiento de los objetivos en relación a la gestión integral del riesgo. • Revisar periódicamente las actividades de control para determinar su efectividad, de ser necesario realizar actualizaciones. • Realizar monitoreo a los riesgos acorde con la política de administración de riesgo establecida para la entidad. • Formular planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados.
Segunda Línea de Defensa Grupo Planeación Estratégica - GRUPL Grupo Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones - SISAM	Asegurar que los controles y procesos de gestión del riesgo de la Primera Línea de Defensa sean apropiados y funcionen correctamente, analizar y consolidar información, que sirvan para definir acciones preventivas frente a cualquier materialización de riesgos.	• Verificación, en el marco de la política de riesgos institucional, que la identificación y valoración del riesgo de la primera línea sea adecuada frente al logro de objetivos y metas. • Verificación de que los responsables estén ejecutando los controles tal como han sido diseñados. • Asesor a la Primera Línea de Defensa en la implementación de la metodología de administración de riesgos dentro de las etapas de identificación, análisis, Definición de Controles y Tratamiento.
Tercera Línea de Defensa Grupo Seguimiento y Evaluación - GRSYE	Realizar Seguimiento a la efectividad de los controles e implementación de controles.	• Realizar recomendaciones frente a la administración de riesgos, con la coordinación de la Oficina de Planeación.

LÍNEAS DE DEFENSA	ROL PRINCIPAL	ACTIVIDADES EN EL SISTEMA DE CONTROL INTERNO (SCI)
	Seguimiento a los planes de mejoramiento.	• Evaluación de la gestión del riesgo de la entidad de forma integral, con énfasis en: • La exposición al riesgo, acorde con los lineamientos y la política institucional. • El cumplimiento legal y regulatorio. • Logro de los objetivos estratégicos o institucionales. • Evaluación de la efectividad de las acciones desarrolladas por la segunda línea de defensa en aspectos como: cobertura de riesgos, cumplimientos de la planificación, mecanismos y herramientas aplicadas, entre otros, y generar observaciones y recomendaciones para la mejora.

Fuente: Manual Operativo del Modelo Integrado de Planeación y Gestión Versión 5

8.8. Materialización

El Gestor de Riesgos del Grupo Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones – SISSAM, realizara seguimiento en la Plataforma Tecnológica SUITE VISION, informando los eventos presentados, realizando informe sobre las consecuencias e impacto que se presentaron dentro de la infraestructura tecnológica, Sistemas de Información, y/o Activos de Información afectados, Igualmente deberá formular las acciones de contingencias que se implementaron frente a materialización del riesgo.

Teniendo en cuenta lo anterior se deberá realizar un análisis, valoración del riesgo, ajustar controles e implementar nuevos si es necesario, en caso de que el riesgo no esté identificado se realizara el proceso de gestión de riesgo (Identificación, Análisis, Valoración y Tratamiento) por parte del Gestor de Riesgo del Grupo SISAM, una vez consolidado, se informara al Grupo de Planeación para el ingreso a la Plataforma Tecnológica SUITE VISION, con el fin de realizar su monitoreo y seguimiento.

Los ajustes, actualización y creación de nuevos riesgos, deberán ser presentado ante el Subcomité de Seguimiento y Evaluación para su aprobación, igualmente ante el Comité Institucional de Gestión y Desempeño para su socialización e implementación.

9. Actividades A Desarrollar Vigencia 2025

Se contemplan en este plan las siguientes actividades a desarrollar durante la vigencia 2025:

Tabla 4. Cuadro de actividades a desarrollar durante la vigencia 2025

Actividades	Productos	Responsable	Fecha Programada	
			Fecha Inicial	Fecha Final
Realizar un análisis periódico de los controles implementados en cada uno de los riesgos.	Informe trimestral de los riesgos que se han mitigados a través de medidas de seguridad.	Área Seguridad de la Información- AREIN	05/03/2025	31/12/2025

Actividades	Productos	Responsable	Fecha Programada	
			Fecha Inicial	Fecha Final
Copia de Seguridad y Recuperación de Datos.	Implementar una estrategia de respaldo de datos y planes de recuperación ante desastres.	Área Seguridad de la Información- AREIN	05/03/2025	31/12/2025
Protección contra Malware y Amenazas Externas.	Implementar soluciones de protección contra malware y antivirus.	Área Seguridad de la Información- AREIN	05/03/2025	31/12/2025
Proceso de gestión y parcheo de vulnerabilidades de sistemas.	Por medio de una aplicación de monitoreo detectar lo que este desactualizado y corregir las novedades encontradas.	Área Seguridad de la Información- AREIN	05/03/2025	31/12/2025

Fuente: Elaboración propia SISAM

10. Indicador

El monitoreo y seguimiento de los riesgos de Seguridad y Privacidad de la Información de la Dirección General de Sanidad Militar DIGSA, se realizara con un indicador de eficacia que permita medir el nivel de cumplimiento de las actividades formuladas, como complemento a estas se implementara dos indicadores, el primero que permite determinar el nivel de implementación de los controles a los riesgos establecidos, el segundo indicador permite determinar la eficiencia en el tratamiento de eventos relacionados la seguridad de la información.

Indicador Eficacia: Cumplimiento de actividades Plan de Tratamiento de Riesgos

$$Eficacia\ Plan\ de\ Tratamiento\ de\ Riesgos = \frac{Numero\ de\ Actividades\ Ejecutadas}{Numero\ de\ Actividades\ Planedas} * 100\% = \%\ Cumplimiento$$

Indicador de Gestión: Tratamientos de eventos relacionados en marco de seguridad y privacidad de la información

Definición: El indicador permite determinar la eficiencia en el tratamiento de eventos relacionados la seguridad de la información. Los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el sistema.

Objetivo: El objetivo del indicador es reflejar la gestión y evolución del modelo de seguridad y privacidad de la información al interior de una entidad

$$Eficiencia\ Tratamiento\ Eventos\ Seguridad\ de\ la\ Información = \frac{Número\ de\ anomalías\ cerradas.}{Número\ total\ de\ anomalías\ encontradas.} * 100\% = \%\ Cumplimiento$$

Indicador de Gestión: Porcentaje de Implementación de Controles

Definición: Grado de avance en la implementación de controles de seguridad.

Objetivo: Busca identificar el grado de avance en la implementación de controles de seguridad

$$Avance\ Implmentación\ Controles = \frac{Número\ de\ Controles\ Implementados}{Número\ de\ Controles\ que\ se\ planearon\ implementar} * 100\% = \%\ Cumplimiento$$

11. Recursos

La Dirección General de Sanidad Militar en el marco de la Gestión de Riesgos de Seguridad y Privacidad de la Información, dispone de los siguientes recursos:

Tabla 5. Cuadro de Recursos

No.	Recursos	Variable
1.	Humanos	El Grupo Sistema Integral de Información– Tecnologías de la Información y las Comunicaciones a través del Área de Seguridad de la Información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la DIGSA en lo concerniente a la seguridad y privacidad de la información.
2.	Técnicos	Guía para la Administración del riesgo y el diseño de controles en entidades públicas, versión 5 del Departamento Administrativo de la Función Pública. Guía para la Administración del Riesgo SSFM DIGSA.MDN-COGFM-PROPLAES-DIGSA-GI.95.1-2
3.	Financieros	Para fortalecimiento en la gestión de riesgos se dispone de proyectos y presupuesto asignado, los cuales se relación en el Plan de Seguridad y Privacidad de la Información.

Fuente: Elaboración propia SISAM

12. Bibliografía

Departamento Administrativo de la Función Pública, Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, versión 5 de diciembre 2020. Bogotá.

Departamento Administrativo de la Función Pública, Guía para la Administración del Riesgo y el diseño de Controles en entidades Públicas, versión 5 de diciembre 2020. Bogotá

Ministerio de las Tecnologías de la Información y Comunicaciones, Guía de Gestión de Riesgos, https://www.mintic.gov.co/gestionti/615/articles- 5482_G7_Gestion_Riesgos.pdf.

Instituto Colombiano de Normas Técnicas y Certificación – ICONTEC. Norma Técnica Colombiana NTC/ISO/31000(2018). Gestión del Riesgo. Bogotá D.C.

Instituto Colombiano de Normas Técnicas y Certificación – ICONTEC. Norma Técnica Colombiana NTC ISO 31000:2018. Gestión del Riesgo. Principios y Directrices. Bogotá D.C.