PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN "PESI"

2025

MINISTERIO DE DEFENSA NACIONAL

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES TICS

GRUPO SEGURIDAD DIGITAL

INTRODUCCIÓN

Los activos de información de la Unidad de Gestión General del Ministerio de Defensa Nacional constituyen uno de los activos de más valor, los cuales soportan su misión y visión; por lo tanto, requieren ser utilizados y manejados dentro de un adecuado entorno de seguridad, cualquiera que sea el medio y el ambiente tecnológico en el que se encuentren.

Así mismo, la Dirección de Tecnologías de la Información y las Comunicaciones es altamente dependiente de sus sistemas de información y de los recursos informáticos, por lo que se constituye en una decisión estratégica implementar un Sistema de Gestión de Seguridad de la Información que permita brindar a los procesos de la entidad y a los usuarios a los cuales les presta servicio de apoyo, niveles apropiados de seguridad y protección de su información.

El diseño, implantación y operación del Plan Estratégico de Seguridad de la Información de la Unidad de Gestión General del Ministerio de Defensa Nacional está directamente relacionado con sus necesidades, objetivos organizacionales, direccionamiento estratégico, estructura, alcance y requerimientos de seguridad.

El Plan Estratégico de Seguridad de la Información está orientado a definir los aspectos necesarios para establecer, operar, mantener y dirigir un sistema efectivo para el tratamiento seguro de la información en la Unidad de Gestión General del Ministerio de Defensa Nacional.

Este documento describe los objetivos y responsabilidades relacionadas con el Modelo de Seguridad y Privacidad de la Información (MSPI), así como los procedimientos de gestión y demás requerimientos del Sistema de Gestión de Seguridad de la Información, con base en las recomendaciones, los requerimientos, controles y objetivos de control especificados en el estándar ISO/IEC 27001:2013.

OBJETIVO GENERAL

Definir una estrategia de seguridad de la información que permita establecer lineamientos en la entidad para el logro de los objetivos estratégicos institucionales garantizando la confidencialidad, integridad y disponibilidad sobre los activos de información.

OBJETIVOS ESPECIFÍCOS

- Definir y establecer la estrategia de seguridad digital de la entidad.
- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

- Disminuir los incidentes cibernéticos que puedan vulnerar las bases de datos y demás activos de información relacionados con la seguridad nacional, pública y ciudadana a cargo de la entidad.

- Incrementar la aplicación de controles para proteger la confidencialidad, integridad, disponibilidad y privacidad de la información de la entidad.

- Afianzar la cultura organizacional frente a la gestión del riesgo de seguridad de la información a través de campañas de sensibilización enfocado al personal que labora en la entidad.

MARCO NORMATIVO

El Plan Estratégico de Seguridad y Privacidad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Decreto 612 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", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.

- Decreto 1874 del 30 de diciembre de 2021, por el cual se modifica la estructura del Ministerio de Defensa Nacional, se crean nuevas dependencias, así como funciones y se dictan otras disposiciones.

- Decreto No.338 del 8 de marzo de 2022, por el cual se adiciona el Titulo 21 a la Parte del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la Seguridad Digital y se dictan otras disposiciones.

- Decreto No. 1263 del 22 de julio de 2022, por el por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública.

- Resolución Número 00500 de marzo 10 de 2021 del Ministerio de tecnologías de la Información y las Comunicaciones, 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 1463 del 28 de marzo de 2022, por la cual se crean y organizan Grupos internos de trabajo del Ministerio de Defensa Nacional – Unidad de Gestión General y se modifica la resolución 0028 del 7 de enero de 2022, en su Artículo 1 se crean Grupos internos de trabajo

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

del Despacho de ministro de Defensa Nacional – Dirección de Tecnologías de la Información y las Comunicaciones.

- Resolución 1621 del 06 de abril de 2022, por la cual se adopta el Modelo Integrado de Planeación y Gestión y se integra el Modelo Estándar de Control Interno, se conforma el Comité Institucional de Gestión y Desempeño y el Subcomité de Coordinación del Sistema de Control Interno en la Unidad de Gestión General del Ministerio de Defensa Nacional y se derogan unas resoluciones.

- Resolución 7870 del 26 de diciembre de 2022, por la cual se emite y adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa, y se dictan otras disposiciones.

- Resolución 4866 del 01 de diciembre de 2023, por la cual se modifica parcialmente la Resolución 1621 de 2022.

- Directiva Presidencial 02 del 24 de febrero de 2022, por la cual se imparten directrices en materia de la Política Pública de Seguridad Digital.

- CONPES 3701 del 14 de julio de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.

- CONPES 3854 del 11 de abril de 2016 POLÍTICA NACIONAL DE SEGURIDAD DIGITAL.

- CONPES 3995 del 01 de julio de 2020 POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL.

- Manual de Gobierno Digital – MINTIC.

- Modelo de Seguridad y Privacidad de la Información – MINTIC.

RESPONSABLES DEL PLAN

Dirección de Tecnologías de la Información TICS – Grupo de Seguridad Digital.

ALCANCE

El Plan Estratégico de Seguridad y Privacidad de la Información, al buscar la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

entidad, comparte el alcance definido dentro de la Política General de Seguridad de la Información, donde se indica que se tendrán en cuenta para la certificación inicial los siguientes procesos identificados en el mapa de procesos vigente de la Unidad de Gestión General del Ministerio de Defensa Nacional:

- Proceso Defensa y Seguridad.
  - Oficina de Respuesta a Incidentes Cibernéticos - CSIRT
  - Dirección de Seguridad Nacional
  - Dirección de Seguridad Pública
  - Dirección de Seguridad Ciudadana

- Proceso Tecnologías de la Información y las Comunicaciones TIC's.
  - Dirección de Tecnologías de la Información y las Comunicaciones - TICS

PROCESOS O DEPENDENCIAS DE APOYO

Las dependencias de apoyo de la Seguridad de la Información en la Unidad de Gestión General del Ministerio de Defensa Nacional se identifican en el Manual de Seguridad de la Información 2024 de acuerdo con las responsabilidades establecidas en el mismo documento. Se establecen las siguientes responsabilidades y dependencias de apoyo:

1. RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN:

1) La responsabilidad final de la protección de los activos de información de la Unidad de Gestión General del Ministerio de Defensa Nacional radica en los propietarios de dichos activos.

2) Adicionalmente, cada persona natural o jurídica que interactúa con los activos de información de la Unidad de Gestión General del Ministerio de Defensa Nacional tiene responsabilidades específicas para garantizar la integridad, confidencialidad y disponibilidad de dichos activos, particularmente sobre aquellos requeridos para el desempeño de sus funciones.

3) Responsabilidades de la alta dirección:
   a. Dar una clara dirección del uso de los activos de información de la Unidad de Gestión General del Ministerio de Defensa Nacional.
   b. Comprometerse y soportar el proceso de seguridad de los activos de información de la Unidad de Gestión General del Ministerio de Defensa Nacional.
   c. Participar en el Comité de gestión y desempeño institucional y apoyar las iniciativas de seguridad que se definan sobre los activos de información.
   d. Aprobar y poner en ejecución las Políticas de Seguridad de Información.
   e. Aprobar y poner en ejecución las iniciativas para la protección de los activos de información, aprobadas por el Comité de gestión y desempeño institucional.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

f. Proveer los recursos financieros requeridos para la apropiada protección de los activos de información.

4) Viceministros, secretarios, directores, jefes de oficina y coordinadores de grupo
   a. Facilitar el desarrollo de programas y/o actividades de formación, inducción, reinducción dirigidos a los colaboradores del Ministerio de Defensa Nacional - Unidad de Gestión General, relacionadas con las actividades de la gestión institucional que fomenten la aplicación y entendimiento del Sistema de Gestión de Seguridad de la Información.
   b. Facilitar la información a los Socios de Negocios (Proveedores de bienes y servicios), relacionada con las actividades de la gestión institucional que fomenten la aplicación y entendimiento del Sistema de Gestión de Seguridad de la Información.
   c. Entender, cumplir y aplicar los requisitos del Sistema de Gestión de Seguridad de la Información en lo que respecta a su rol.
   d. Reconocer la independencia y autoridad de la Función de Cumplimiento (Oficina de Relación con el Ciudadano) en su rol de asegurar la implementación efectiva y operación continua del Sistema de Gestión de Seguridad de la Información.
   e. Actuar en el marco de la ética institucional, legal y del Código de Integridad.
   f. Adelantar los trámites de debida diligencia que correspondan de acuerdo con su rol y las funciones del cargo.
   g. Realizar requerimientos relacionados con el desarrollo de las acciones de debida diligencia en los procesos desarrollados en sus dependencias.

5) Dirección de Tecnologías de la Información y las Comunicaciones
   a. Promover el cumplimiento por parte del personal bajo su responsabilidad de las Políticas de Seguridad de la Información.
   b. Implementar y administrar las herramientas tecnológicas para el cumplimiento de las Políticas de Seguridad de Información.
   c. Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de Seguridad de Información.
   d. Diseñar, desarrollar, instalar y mantener las aplicaciones bajo su responsabilidad de acuerdo con la metodología establecida e incluyendo los controles de Seguridad de Información desde el diseño.
   e. Establecer, documentar y dar mantenimiento a los procedimientos de seguridad que apliquen para la plataforma de tecnologías de información administrada por esta Dirección.
   f. Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo.
   g. Establecer y dar mantenimiento a los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.
   h. Monitorear y evaluar los procesos o actividades sobre las plataformas tecnológicas, delegados en terceros.
   i. Implementar y administrar los controles de seguridad sobre los datos y conexiones de la red de datos bajo su administración.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

j. Desarrollar e implementar programas de capacitación y entrenamiento que incluyan temas relevantes y pertinentes sobre seguridad de información.
k. Custodiar la información y los medios de almacenamiento bajo su responsabilidad.
l. Operar y administrar los recursos de cómputo, de red y de software bajo su responsabilidad.

6) Servidores públicos no directivos y contratistas de prestación de servicios
   a. Cumplir con los lineamientos, códigos, procedimientos y acuerdos institucionales relacionados con la prohibición de cualquier práctica descrita en el Sistema de Gestión de Seguridad de la Información.
   b. Entender, cumplir y aplicar los requisitos del Sistema de Gestión de Seguridad de la Información en lo que respecta a su rol.
   c. Adelantar los trámites de debida diligencia que correspondan de acuerdo con su rol y las funciones del cargo.
   d. Reconocer la independencia y autoridad de la Función de Cumplimiento (Oficina de Relación con el Ciudadano) en su rol de asegurar la implementación efectiva y operación continua del Sistema de Gestión de Seguridad de la Información
   e. Proporcionar la información a las partes interesadas relacionadas con las actividades de la gestión institucional que fomenten la aplicación y entendimiento del Sistema de Gestión de Seguridad de la Información.
   f. Asistir a las capacitaciones que traten del Sistema de Gestión de Seguridad de la Información (ISO 27001:2013.

7) Responsabilidades de los dueños de los procesos.
   a. Definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados en su proceso, incluyendo aquellas actividades que sean consideradas como controles de seguridad de la información dentro de dichos procedimientos.

8) Responsabilidades de los propietarios de los activos de información.
   a. Nombrar gestor de activos de información, quien será el encargado de la identificación, clasificación de activos de información, riesgos y planes de tratamiento.
   b. Clasificar sus activos de información de acuerdo con los requerimientos de confidencialidad, integridad y disponibilidad.
   c. Definir los acuerdos de niveles de servicio para recuperar sus activos de información y sistemas críticos e identificar los impactos para la Unidad de Gestión General del Ministerio de Defensa en caso de una interrupción extendida.
   d. Definir los requerimientos de continuidad y de recuperación en caso de desastre.
   e. Realizar un análisis anual de riesgos para determinar el grado de exposición a las amenazas vigentes y confirmar los requerimientos de confidencialidad, integridad y disponibilidad relacionados con sus activos de Información.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

f. Definir los requerimientos de seguridad para los activos de información bajo su responsabilidad para que se les proporcione un nivel adecuado de protección en conformidad con los estándares, políticas y procedimientos de seguridad de información.
g. Comunicar sus requerimientos de seguridad de la información al coordinador del Grupo de Seguridad de Digital.
h. Determinar y autorizar todos los privilegios de acceso a sus activos de información.
i. Comunicar al Grupo de Seguridad Digital sus requerimientos en capacitación sobre seguridad de información.
j. Revisar los registros y reportes de auditoría para asegurar el cumplimiento con las restricciones de seguridad para sus activos de información. Estas revisiones podrán realizarse en coordinación con el custodio del activo; sin embargo, se deben verificar los resultados de las revisiones y reportar cualquier situación que involucre un incumplimiento o violación a la seguridad de Información, de acuerdo con el procedimiento de gestión de incidentes de seguridad.
k. Participar en la resolución de los incidentes relacionados con el acceso no autorizado o mala utilización de los activos de información bajo su responsabilidad, incluyendo los incumplimientos a la disponibilidad, confidencialidad e integridad.

9) Responsabilidades comunes para todos los funcionarios, contratistas y terceros de la Unidad de Gestión General del Ministerio de Defensa Nacional.
   a. Cumplir fielmente las Políticas de Seguridad de Información.
   b. Velar por el fiel cumplimiento de las políticas de seguridad de información dentro de su entorno laboral inmediato.
   c. Reportar, a la mayor brevedad posible y a través de los canales establecidos, la sospecha u ocurrencia de eventos considerados incidentes de seguridad de información, incluyendo entre otros, la mala utilización de recursos, uso ilegal del software, virus, evidencia de que alguien irrumpa, etc.
   d. Emitir a la autoridad inmediata superior sus sugerencias para la mejora en el manejo seguro de los activos de Información.
   e. Utilizar los sistemas del Ministerio de Defensa Nacional y el acceso a la red únicamente para propósitos indicados en las Políticas de Seguridad de la Información.
   f. Incorporar la Seguridad de Información como parte de las actividades y tareas bajo su responsabilidad.
   g. Conocer las directrices de protección de los activos de información que utilicen.
   h. Utilizar únicamente software y demás recursos tecnológicos autorizados por el Ministerio de Defensa Nacional.

10) Responsabilidades de supervisores de contratos.
   a. Reportar a la Dirección de Tecnologías de la Información y las Comunicaciones cualquier novedad sobre el personal de terceros o contratistas que acceden a la plataforma tecnológica del Ministerio de Defensa Nacional para tomar las medidas necesarias que mitiguen riesgos de seguridad de la información.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

2. DEPENDENCIAS DE APOYO EN SEGURIDAD DE LA INFORMACIÓN:

1) Dirección de Gestión del Talento Humano.
   a. Seleccionar y contratar el personal de la Unidad de Gestión General del Ministerio de Defensa Nacional teniendo en cuenta los requerimientos de las Políticas de Seguridad de la Información.
   b. Incluir en los contratos cláusulas de confidencialidad y no divulgación de la información, así como la obligatoriedad en el cumplimiento de las políticas, procedimientos, restricciones y controles de Seguridad de la Información.
   c. Asegurar que todo el personal que tenga la autorización de utilizar los activos de información de la Unidad de Gestión General del Ministerio de Defensa Nacional haya firmado un convenio de responsabilidad por el buen uso de estos.
   d. Informar a la Dirección de Tecnologías de la Información y las Comunicaciones la desvinculación de cualquier empleado y demás novedades de personal con el fin de que se tomen las medidas necesarias para evitar riesgos de seguridad de información.
   e. Definir e implementar la estrategia de concientización y capacitación en seguridad de la información para los funcionarios, así como contratistas y demás terceros cuando aplique.
   f. Exigir a los funcionarios que se desvinculan de la Unidad de Gestión General del Ministerio de Defensa Nacional el paz y salvo con el Almacén General y la Dirección de Tecnologías de la Información y las Comunicaciones, antes de formalizar dicha desvinculación.

2) Oficina de Control Interno Sectorial.
   a. La Oficina de Control Interno Sectorial, a través del Grupo de Evaluación y Auditoría, validará la aplicación y cumplimiento de las Políticas de Seguridad de Información definidas en este manual, la aplicación de controles sobre los activos de información propiedad de la Unidad de Gestión General del Ministerio de Defensa Nacional y los requerimientos del Sistema de Gestión de Seguridad de la Información.
   b. Revisar controles de auditoría sobre los sistemas de información y demás elementos de la plataforma tecnológica.
   c. Auditar a discreción el proceso de Seguridad de Información o por pedido de los dueños de los activos de información.

3) Oficina de Control Interno Disciplinario.
   a. Adelantar los trámites pertinentes al proceso disciplinario derivados de quejas y/o reportes por situaciones del SGSI.
   b. Realizar los reportes a organismos pertinentes, cuando corresponda, como resultado del proceso disciplinario adelantado por actos de SGSI
   c. Adelantar las investigaciones pertinentes por conductas relacionadas con actos de SGSI.
   d. Requerir información correspondiente al funcionamiento del Sistema de Gestión de Seguridad de la Información, así como la que considere pertinente en el desarrollo de investigaciones disciplinarias.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

4) Dirección Sectorial de Comunicaciones.
   a. Diseñar, formular, implementar y administrar los contenidos de la Estrategia de Comunicaciones del Sistema de Gestión de Seguridad de la Información.
   b. Promover y desarrollar continuamente la implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información.
   c. Crear y administrar el módulo Sistema de Gestión de Seguridad de la Información en la página web del Ministerio de Defensa Nacional.
   d. Elaborar y diseñar piezas gráficas, contenido audiovisual para llevar a cabo la comunicación continua de la Estrategia de Comunicaciones del Sistema de Gestión de Seguridad de la Información en la Unidad de Gestión General.
   e. Promover la difusión de lineamientos, campañas, estrategias y sensibilización al interior de la Unidad de Gestión General.

5) Oficina de Respuesta a Incidentes Cibernéticos – CSIRT
   a. Formular e implementar el Plan Estratégico Sectorial en materia de capacidades en Ciberseguridad y Ciberdefensa del Sector Defensa, hacer seguimiento, medición, análisis y evaluación.
   b. Coordinar las capacidades de ciberseguridad y ciberdefensa con la Dirección de Seguridad Nacional y los organismos del Sector Defensa y otros sectores.
   c. Formular e implementar las políticas de ciberseguridad y ciberdefensa de la infraestructura crítica del Sector Defensa, con la cooperación de los organismos de seguridad del Sector, hacer seguimiento, medición, análisis y evaluación.
   d. Generar e implementar los protocolos, lineamientos, guías, estándares, buenas prácticas y recomendaciones de ciberseguridad y ciberdefensa para el Sector Defensa y hacer su seguimiento, medición, análisis y evaluación.
   e. Definir acciones, servicios de prevención, concientización y sensibilización ante amenazas cibernéticas y dar respuesta frente a incidentes en esta materia en el Sector Defensa.
   f. Cooperar con los organismos de seguridad e investigación del Estado en la prevención e investigación de delitos donde medien las tecnologías de la información y las comunicaciones.
   g. Formular e implementar planes, programas, proyectos y acciones que permitan generar y producir conocimiento relativo a la ciberseguridad y ciberdefensa para el Sector Defensa.
   h. Generar cultura en el Sector Defensa para crear, conservar, compartir, difundir, reconocer y valorar el conocimiento relativo a la ciberseguridad y ciberdefensa y utilizar herramientas para su apropiación, seguimiento, medición, análisis y evaluación.
   i. Coordinar y actuar como punto de contacto internacional con homólogos de otros países y con organismos internacionales comprometidos con la ciberseguridad y la ciberdefensa.
   j. Gestionar y establecer mecanismos de prevención y control a los incidentes cibernéticos que puedan ocurrir en Ministerio de Defensa Nacional y servir de punto focal especializado del Sector Defensa.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

k. Promover dentro de las entidades del Sector Defensa, el reporte obligatorio de incidentes cibernéticos, ofreciendo garantías de confidencialidad, privacidad, y beneficios de los reportes.
l. Informar a los miembros del ecosistema cibernético del Sector Defensa acerca de las nuevas vulnerabilidades, advertencias y descubrimientos que afecten la seguridad cibernética.
m. Coordinar con la Dirección de Seguridad Nacional y organismos del Sector, la respuesta a incidentes cibernéticos de seguridad y defensa e implementar la infraestructura necesaria y hacer seguimiento a la gestión relacionada con el riesgo en estas materias.

6) Director de Seguridad Nacional
a. Diseñar políticas y programas para mantener la seguridad de la infraestructura estratégica física y cibernética de la Nación.
b. Formular políticas y programas en materia de seguridad nacional y de infraestructura estratégica de la Nación, hacer las coordinaciones para su debida ejecución, consolidar los resultados obtenidos y hacer seguimiento y análisis de acuerdo con los lineamientos impartidos en la Política de Defensa y Seguridad.
c. Identificar requerimientos de los sectores económicos en materia de seguridad, tramitarlos con las dependencias competentes y hacer seguimiento a su atención oportuna.
d. Canalizar los requerimientos en temas de seguridad y defensa de la infraestructura estratégica física y cibernética de la nación y coordinar con las dependencias del Ministerio de Defensa Nacional, entidades gubernamentales y privadas la adopción de estrategias, planes y programas para su debida protección.
e. Dirigir y liderar la ejecución de los programas y directrices del Ministerio de Defensa Nacional en materia de protección a la infraestructura estratégica gubernamental, minera, energética, de hidrocarburos, vial, de transporte, de telecomunicaciones y agroindustrial del país en el ámbito físico y cibernético.
f. Articular las acciones de seguridad requeridas para los procesos electorales, atendiendo los requerimientos de los entes competentes y de la Comisión Nacional para la Coordinación y Seguimiento de los Procesos Electorales.
g. Elaborar planes, programas y propuestas de seguridad con el sector público y privado para la mitigación del riesgo de seguridad que pueda afectar la infraestructura estratégica del país.
h. Contribuir con el diseño y la formulación de políticas, estrategias, planes y programas relacionados con ciberseguridad y ciberdefensa y hacerle el seguimiento, en coordinación con las entidades competentes.
i. Dirigir la consolidación de información que debe ser rendida a las dependencias competentes del Ministerio de Defensa Nacional para la estructuración de las políticas de su competencia.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

j. Liderar, impulsar y promover el análisis de las temáticas de seguridad nacional, protección de la soberanía nacional, la integridad territorial, la infraestructura crítica, y la estabilidad de las instituciones del Estado.

7) Dirección de Seguridad Publica
   a. Diseñar y formular políticas, estrategias, planes y programas para apoyar el desarrollo del país con enfoque de consolidación territorial, coordinar, realizar seguimiento y evaluación de la acción integral que se realiza desde el Sector Defensa, en concordancia con la Política de Defensa y Seguridad.
   b. Apoyar la participación del Sector Defensa en las instancias bilaterales o multilaterales en las que se promuevan acciones para luchar contra las amenazas a la seguridad pública.
   c. Liderar y promover el análisis de las temáticas de la seguridad pública y la lucha contra las amenazas que la afecten.

8) Dirección de Seguridad Ciudadana
   a. Diseñar, formular y monitorear las políticas, estrategias, planes de acción, programas, proyectos y lineamientos generales, relacionados con la seguridad ciudadana, en coordinación con las demás entidades competentes.
   b. Apoyar, la participación del Sector Defensa, en las instancias territoriales a nivel nacional, bilaterales o multilaterales, para promover acciones contra los delitos y fenómenos que afectan la seguridad ciudadana.
   c. Asesorar al Viceministerio para las Políticas de Defensa y Seguridad, en su gestión en las instancias relacionadas con Seguridad Ciudadana.

9) Dirección de Planeación y Presupuesto
   a. Liderar la elaboración del Plan Estratégico Sectorial y del Plan Estratégico Institucional, así como hacer el seguimiento periódico de sus avances.
   b. Emitir lineamientos para la implementación del Modelo de Operación por Procesos del Ministerio de Defensa-Unidad de Gestión General y del Modelo Integrado de Planeación y Gestión en el Ministerio de Defensa y el Sector.
   c. Fomentar la cultura de mejoramiento continuo en los Sistemas de Gestión y Desempeño Institucional en el Ministerio de Defensa Nacional y el Sector.
   d. Implementar, mantener y mejorar los sistemas de gestión bajo estándares nacionales e internacionales y el Modelo Integrado de Planeación y Gestión, que sean adoptados por el Ministerio de Defensa-Unidad de Gestión General.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

CONTENIDO TEMÁTICO:

1. DIAGNÓSTICO

La medición del estado actual de la implementación del SGSI se realiza de acuerdo con el autodiagnóstico de seguridad y privacidad de la información, la evaluación de FURAG en cuanto a la política de Seguridad Digital y el desarrollo de la cultura de seguridad de la información.

A continuación, se muestra el resultado de la evaluación de madurez del Modelo de Seguridad y Privacidad de la Información (MSPI) identificado en el documento de autodiagnóstico, apoyados en la herramienta "INSTRUMENTO DE EVALUACIÓN MSPI de MinTIC, por cada uno de los dominios definidos en dicho modelo, y realizando un comparativo del avance del año 2024 con respecto al año 2023.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	78	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	77	100	GESTIONADO
A.9	CONTROL DE ACCESO	79	100	GESTIONADO
A.10	CRIPTOGRAFÍA	60	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	80	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	86	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	80	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	80	100	GESTIONADO
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	80	100	GESTIONADO
A.18	CUMPLIMIENTO	80	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		80	100	GESTIONADO

Tabla 1 Evaluación de efectividad de controles 2023
Fuente: instrumento de evaluación de MSPI 2023 (Modelo de Seguridad y Privacidad de la Información) MinDefensa

Para el estado actual de la entidad respecto al sistema de gestión de seguridad de la información, y apoyados en la herramienta "INSTRUMENTO DE EVALUACIÓN MSPI (2024)", se obtuvieron los resultados del análisis de brecha sobre la efectividad de los controles con los siguientes resultados:

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	61	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	84	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	75	100	GESTIONADO
A.9	CONTROL DE ACCESO	74	100	GESTIONADO
A.10	CRIPTOGRAFÍA	70	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	100	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	83	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	79	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	56	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	100	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	63	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	80	100	GESTIONADO
A.18	CUMPLIMIENTO	97,5	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		79	100	GESTIONADO

Tabla 2 Evaluación de efectividad de controles 2024
Fuente: instrumento de evaluación de MSPI 2024 (Modelo de Seguridad y Privacidad de la Información) MinDefensa

Teniendo en cuenta que para la vigencia 2024 se mantuvo el alcance del sistema de gestión de seguridad de la información, se evidencia que la calificación, con respecto a la obtenida en el período 2023, disminuyó en un punto y la calificación en algunos de los dominios, de la norma ISO27001, fue más baja con respecto a la vigencia inmediatamente anterior, principalmente:

- A5 Políticas de Seguridad de la Información: de 100 bajo a 90
- A.6 Organización de Seguridad de la información: de 80 bajó a 61
- A.7 Seguridad de los recursos humanos: de 78 incrementó a 84
- A.10 Criptografía: de 60 incrementó a 70
- Los demás dominios se mantuvieron, aunque algunos se encuentran por debajo de 80.

Por lo anterior, se debe seguir trabajando en los dominios que se encuentran por debajo de 80:

- A.6 Organización de la Seguridad de la Información
- A.8 Gestión de Activos
- A.9 Control de Acceso
- A10 Criptografía
- A.13 Seguridad de las Comunicaciones
- A.14 Adquisición, desarrollo y mantenimiento de sistemas
- A.16 Gestión de incidentes de Seguridad de la Información

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

A continuación, se muestra la brecha del sistema de gestión de seguridad de la información (SGSI) con respecto a la norma ISO 27001:2013:

Ilustración 1 Brechas de Seguridad
Fuente: instrumento de evaluación de MSPI 2024 (Modelo de Seguridad y Privacidad de la Información) MinDefensa

A partir de la evaluación de la calificación de MSPI (2024), se identifica que, aunque el dominio de Criptografía disminuyó su calificación y sigue presentando una calificación por debajo del punto objetivo (de 80 a 100), esto debido a la baja efectividad de controles criptográficos, los cuales repercuten en la clasificación global y a la ampliación del alcance del sistema. Lo anterior, debido al recorte presupuestal que al interior del ministerio se dio durante la vigencia 2024 y se dio prioridad a otras plataformas de seguridad.

Las dependencias que conforman la Unidad de Gestión General del Ministerio de Defensa Nacional en coordinación con la Dirección de Tecnologías de la Información y las Comunicaciones TICS, líder del proceso del Sistema de Gestión de Seguridad de la Información (SGSI), bajo el marco de Política de Seguridad Digital y del modelo MSPI de MinTIC, y cuya responsabilidad es capacitar y acompañar en la gestión de riesgos de seguridad a todos los gestores nombrados por cada Dirección, han trabajado en la identificación de activos de información, los riesgos asociados a los mismos y en la implementación de planes de tratamiento. Esta información se encuentra de manera detallada en la matriz de gestión de riesgos de seguridad de la información.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

De **1497** activos identificados, **636** son de información y **150** de servicio, mientras que los **711** restantes son activos de soporte los cuales no tienen un riego inherente (riesgo sin aplicar un control).

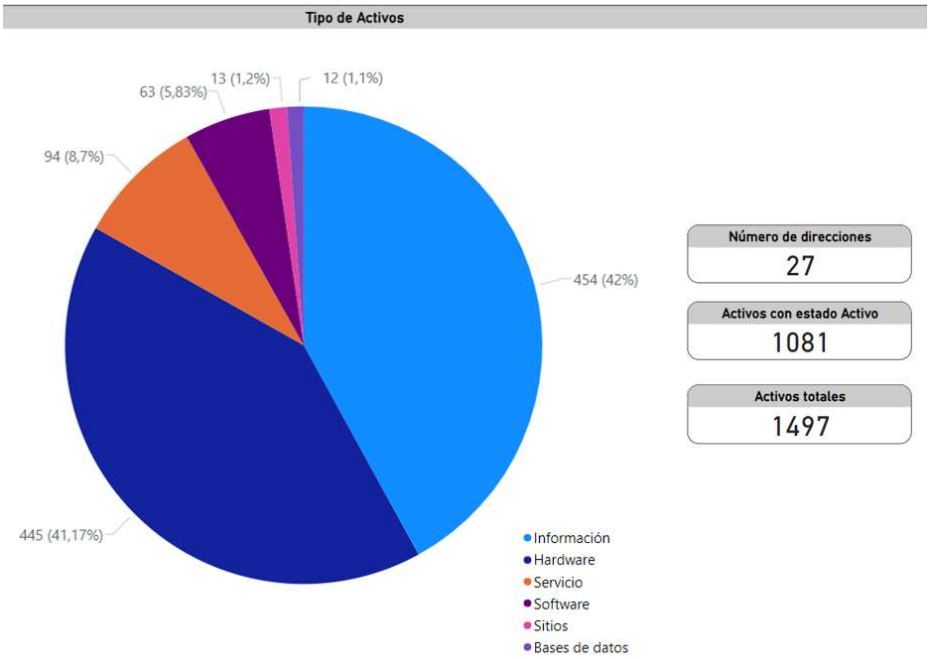

Ilustración 2. Tipos de activos
Fuente: plataforma segin.mindefensa.col

En la siguiente ilustración se presenta la discriminación de los riesgos inherentes y residuales identificados por nivel de riesgo así:

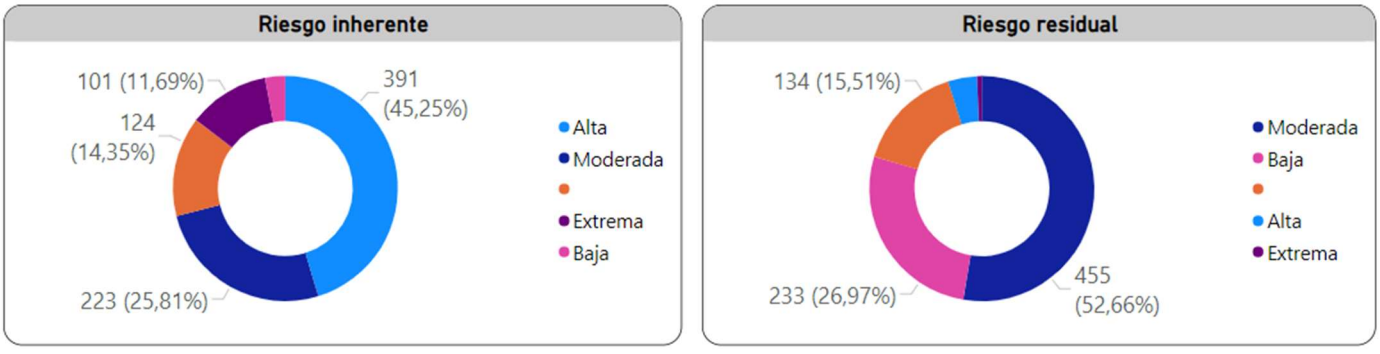

Ilustración 3. Conteo de valoraciones de riesgos.
Fuente: plataforma segin.mindefensa.col

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

La Dirección de Tecnologías de la Información y las Comunicaciones como una de las líneas de defensa de riesgos de seguridad de la información por cuanto implementa controles técnicos, tecnológicos y culturales, brinda acompañamiento a los procesos de la entidad para implementar la metodología de gestión del riesgo de la UGG, identificando los activos de información con criticidad más alta por dependencia y así establecer las causas, efectos, controles y acciones de tratamiento de los mismos.

2. DESARROLLO DEL PLAN

2.1. ESTRATEGIA DE SEGURIDAD DIGITAL

LA UGG establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira en torno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse.

Por tal motivo, LA ENTIDAD define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

Ilustración 4 Ejes Estrategia de Seguridad Digital
Fuente: https://gobiernodigital.mintic.gov.co/692/w3-article-150511.html

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

2.2. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

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 resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se mantenga 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 UGG 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 se 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, identificados en el Plan de Comunicaciones de Seguridad Digital.
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 UGG, se pueden subdividir en controles tecnológicos, técnicos y culturales.
Gestión de incidentes	Fortalecer una administración de incidentes de seguridad de la información, a través de la oficina de respuesta a incidentes cibernéticos (CSIRT defensa), 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 UGG.

Tabla 2 Estrategias específicas de seguridad digital
Fuente: elaboración propia MinDefensa
Formato MinTIC https://gobiernodigital.mintic.gov.co/692/w3-article-150511.html

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

2.3. PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, la UGG define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI), bajo el Modelo de Seguridad y Privacidad de la Información - MSPI como habilitador de la política de *Seguridad* Digital - ***MIPG***:

ESTRATEGIA / EJE	**PROYECTO**	**PRODUCTOS ESPERADOS**
Implementar el Modelo de Seguridad y Privacidad de la Información - MSPI como habilitador de la política de Seguridad Digital: **MIPG** / *LIDERAZGO DE SEGURIDAD DE LA INFORMACIÓN*	PROYECTO 1: *Fortalecer la Política de Seguridad Digital*: Ampliar el alcance y mejoramiento continuo del SGSI, bajo el Modelo de Seguridad y Privacidad de la Información - MSPI.	
	1. Evaluar el nivel de madurez MSPI con respecto a la norma NTC/ISO 27001:2022.	1. Informe y Documento de análisis GAP del MSPI actual con respecto a la norma NTC/ISO 27001:2022 y recomendaciones para su actualización.
	2. Incluir y acompañar en la preparación a los procesos que estarán adicionales en la ampliación del alcance a la certificación del SGSI para la UGG.	2. Informe para aprobación del Comité de Gestión de Desempeño Institucional donde se identifican los procesos de la UGG que estarían listos para la certificación en la norma NTC/ISO 27001:2022.
	PROYECTO 2: *Fortalecer la Política de Seguridad Digital*: Actualizar las Políticas sectoriales de Seguridad Digital,	

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

ESTRATEGIA / EJE	**PROYECTO**	**PRODUCTOS ESPERADOS**
	Ciberseguridad y Servicios en Nube. 1. Solicitar a través de oficio, el nombramiento de los responsables de cada una de las entidades del sector defensa para asistir a las mesas de trabajo de actualización de las políticas de tecnología. 2. Realizar las mesas de trabajo de actualización de las políticas de tecnología con los representantes nombrados por cada una de las entidades sectoriales. 3. Generar proyecto de resolución para la actualización de las Políticas de Tecnología para el Sector Defensa.	1. Oficio dirigido a los directores de tecnología de cada una de las entidades del sector defensa. 2. Informe de actualización de las Políticas de Tecnología para el Sector Defensa y actas de reunión. 3. Proyecto de Resolución.
Implementar el Modelo de Seguridad y Privacidad de la Información - MSPI como habilitador de la política de Seguridad Digital: **MIPG** / *GESTIÓN DE RIESGOS*	PROYECTO 3: Planes de tratamiento de riesgos de Seguridad de la Información. 1. Actualizar, valorar y clasificar los activos de información de cada una de las dependencias de la UGG. 2. Actualizar, valorar y clasificar los riesgos asociados a los activos de información. 3. Definir los nuevos planes de tratamiento de riesgos de seguridad para los	1. Reporte de activos de información actualizados, obtenido de la plataforma GRC. 2. Matriz de riesgos de seguridad digital, obtenida de la plataforma GRC. 3. Plan de tratamiento de riesgos, obtenido de la

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

ESTRATEGIA / EJE	**PROYECTO**	**PRODUCTOS ESPERADOS**
	riesgos identificados. PROYECTO 4: Participar en las mesas de trabajo para el diseño e implementación del BCP de la UGG, en el que se incluya el DRP tecnológico. 1. Realizar viabilidad y plan de trabajo con las dependencias responsables del BCP (Plan de Continuidad del Negocio) con el fin de incluir el DRP (Plan de Recuperación de Desastres Tecnológico). 2. Rediseñar la estrategia DRP de servicios críticos en la UGG, alineados el BCP institucional. 3. Estimar los costos para la implementación de la estrategia DRP de los servicios críticos en la UGG.	plataforma GRC. 1. Informe donde se identifican las estrategias aportadas por cada una de las dependencias del Ministerio de Defensa Nacional y su viabilidad de implementación. 2. Informe de rediseño de estrategias DRP. 3. Informe de estimación de costos para la implementación de la estrategia DRP de los servicios críticos en la UGG.
Implementar el Modelo de Seguridad y Privacidad de la Información - MSPI como habilitador de la política de Seguridad Digital: **MIPG** / *CONCIENTIZACIÓN*	PROYECTO 5: Reevaluación del Plan de Comunicaciones del SGSI en el plan de TICS. 1. Actualizar el Plan de Comunicaciones en el que se establecen mecanismos de capacitación y sensibilización en seguridad digital y ciberseguridad, gobierno y transformación digitales, plataformas de	1. Plan de Comunicaciones actualizado para la DTICS.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

ESTRATEGIA / EJE	**PROYECTO**	**PRODUCTOS ESPERADOS**
	infraestructura y arquitectura empresarial. 2. Campaña día de la DTICS, en la que se presentan las herramientas de uso general y nuevas tecnologías para todos los funcionarios de la UGG. 3. Realizar campañas de socialización para el uso y apropiación de herramientas tecnológicas (almacenamiento y correo electrónico) que tiene el ministerio para sus usuarios. 4. Sensibilizar al personal de la UGG en la detección y reporte de posibles incidentes cibernéticos, así como en ciberseguridad y ciberdefensa. CSIRT.	2. Evidencias de las actividades desarrolladas (Comunicados oficiales, correos electrónicos, piezas graficas, presentaciones de sensibilización, encuestas). 3. Certificaciones de cursos 4. Sesiones de capacitación desarrolladas.
Implementar el Modelo de Seguridad y Privacidad de la Información - MSPI como habilitador de la política de Seguridad Digital: **MIPG** / *IMPLEMENTACIÓN DE CONTROLES*	CONTROL 1: Adopción de agentes de Inteligencia Artificial para controlar aspectos de seguridad digital en la UGG. 1. Realizar la preparación en aspectos de seguridad para la adopción de los agentes de Inteligencia Artificial en la UGG. 2. Apoyar en la sensibilización del uso de los agentes de Inteligencia Artificial en la UGG.	1. Informe de aspectos de seguridad en la adopción de Inteligencia Artificial. 2. Evidencias de socialización de IA en la UGG correos electrónicos, piezas graficas,

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

ESTRATEGIA / EJE	**PROYECTO**	**PRODUCTOS ESPERADOS**
		presentaciones de sensibilización, encuestas).
	3. Realizar un plan de despliegue de IA para la UGG.	3. Documento de despliegue para la Adopción de IA en la UGG.
	CONTROL 2: Guía Metodológica para el Desarrollo de Software 1. Desarrollar las etapas de Planificación, Análisis de requerimientos y Diseño.	1. Informe del desarrollo de las etapas de Planificación, Análisis de requerimientos y Diseño.
	2. Desarrollar las etapas de Prototipado, Revisión y Desarrollo.	2. Informe del desarrollo de las etapas de Prototipado, Revisión y Desarrollo.
	3. Desarrollar las etapas de Pruebas, Implementación, Mantenimiento y Desmantelamiento.	3. Informe del desarrollo de las etapas de Pruebas, Implementación, Mantenimiento y Desmantelamiento.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

ESTRATEGIA / EJE	**PROYECTO**	**PRODUCTOS ESPERADOS**
Implementar el Modelo de Seguridad y Privacidad de la Información - MSPI como habilitador de la política de Seguridad Digital: **MIPG** / *GESTIÓN DE INCIDENTES*	PROYECTO 6: Fortalecer la Ciberseguridad y Ciberdefensa en el sector Defensa 1. Realizar una guía de prevención, respuesta y recuperación ante presuntos ataques de RANSOMWARE. 2. Realizar informe de eventos cibernéticos maliciosos en el sector Defensa y Seguridad. 3. Realizar una guía de buenas prácticas para la articulación interinstitucional en materia de ciberseguridad y ciberdefensa para el sector. 4. Realizar un ejercicio de ciberseguridad y ciberdefensa técnico - estratégico que permita el fortalecimiento de las capacidades cibernéticas del Sector Defensa.	1. Guía para prevenir ataque de RANSOMWARE. 2. Informe de eventos cibernéticos. 3. Guía de buenas prácticas para la Articulación Interinstitucional Cibernética. 4. Informe ejecutivo con el resultado del ejercicio. (Formato informe DP-F-003)

2.4. CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

A continuación, se establece el cronograma de actividades donde se evidencia como se llevarán a cabo cada uno de los proyectos previstos. Las actividades se desarrollarán durante la vigencia 2024.

Se anexa el Cronograma PESI 2025, de acuerdo con el formato establecido en el ministerio para este fin (**DP-F-026 Formato Cronograma**).

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

3. MONITOREO Y SEGUIMIENTO

El monitoreo del Plan Estratégico de Seguridad y Privacidad de la Información se realiza mediante el uso de las siguientes herramientas:

1. FURAG
Se realiza el diligenciamiento del cuestionario FURAG para establecer el grado de madurez en la implementación de las diferentes políticas.

2. INSTRUMENTO DE EVALUACIÓN MSPI de MinTIC.
Apoyados en la herramienta "INSTRUMENTO DE EVALUACIÓN MSPI" se obtienen los resultados del análisis de brecha sobre la efectividad de los controles, realizado anualmente.

3. MATRIZ GAP
Se realiza el diligenciamiento de la matriz GAP del MSPI para las dependencias del alcance para establecer las brechas de implementación del SGSI.

4. INDICADORES
Se identifican 3 indicadores de seguimiento como parte de la implementación de la política de Seguridad Digital, así:

Nombre Indicador	**Descripción**
CULTURA EN SEGURIDAD DE LA INFORMACIÓN	Incrementar la cultura de seguridad de la información en el talento humano y las partes interesadas, a través de la gestión del riesgo y la mejora continua.
GESTIÓN DE LINEAS BASE DE SEGURIDAD	Determinar la aplicación de controles para proteger la confidencialidad, integridad, disponibilidad y privacidad de la información de la Unidad de Gestión General del Ministerio de Defensa Nacional
INCIDENTES DE SEGURIDAD	Fortalecer la capacidad en la gestión de los incidentes que puedan vulnerar los activos de la información, relacionados con la seguridad y defensa a cargo de la Unidad de Gestión General del Ministerio de Defensa Nacional

Tabla 3: Definición INDICADORES de Seguridad Digital de la Unidad de Gestión General del Ministerio de Defensa Nacional 2023
Fuente: elaboración propia MinDefensa

Estos indicadores se encuentran registrados en la plataforma SUITEV para su seguimiento por la Alta Dirección, como se muestra en la siguiente ilustración:

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

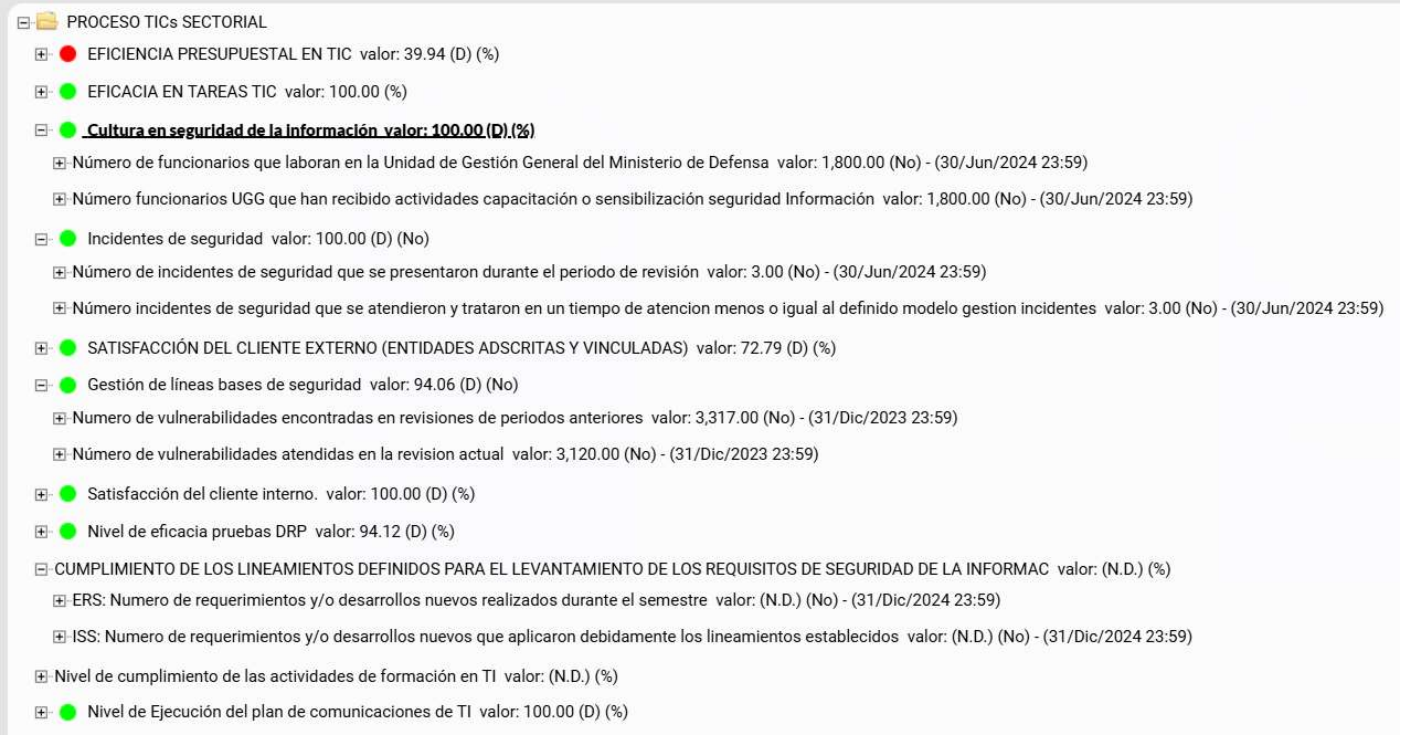

Ilustración 4. INDICADORES Política Seguridad Digital vigencia 2024 de la Unidad de Gestión General del Ministerio de Defensa Nacional
Fuente: elaboración propia MinDefensa. http://suitev.mindefensa.col:9090/suiteve/

3.1. ANÁLISIS PRESUPUESTAL:

Con el fin de establecer y manifestar su compromiso con el Sistema de Gestión de Seguridad de la Información, la alta dirección de la Unidad de Gestión General del Ministerio de Defensa Nacional ha asignado los recursos necesarios para la implementación, operación, mantenimiento y mejora del Sistema, de sus políticas y procedimientos de seguridad; así mismo, se hace responsable por observar su cumplimiento por parte de los funcionarios de la entidad, contratistas y demás terceros.

Como Dirección de Tecnologías de la Información y las Comunicaciones se espera formular un proyecto de inversión que cubra todas las necesidades durante el próximo cuatrienio de acuerdo con lo recomendado por el Departamento Nacional de Planeación con un horizonte del 2024 al 2026, consolidando las necesidades de los proyectos actuales presentados ante el Comité Funcional de Inversión realizado en 2023 teniendo en cuenta las siguientes necesidades:

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

Proyecto	2023	2024	2025	2026	Total
	Necesidad Mínima (millones $)	Necesidad Mínima (millones $)	Necesidad Mínima (millones $)	Necesidad Mínima (millones $)	Necesidad Mínima (millones $)
Fortalecimiento de los servicios Tecnológicos de la Unidad de Gestión General del Ministerio de Defensa Nacional.	**15.268**	**28.700**	**20.210**	**20.570**	**64.538**
Total	**15.268**	**28.700**	**20.210**	**20.570**	**64.538**

Tabla 4: Fortalecimiento de los servicios tecnológicos (incluido Seguridad Digital) de la Unidad de Gestión General del Ministerio de Defensa Nacional-horizonte 2023-2026. Fuente: elaboración propia MinDefensa

3.2. ANÁLISIS CUMPLIMIENTO PLAN

La Alta Dirección demostrará su compromiso a través del seguimiento de la implementación de las políticas establecidas en el Modelo Integrado de Planeación y Gestión (MIPG), dentro de las cuales se encuentra la Política de Seguridad Digital, para lo cual se dispone de la plataforma de servicios SUITEV que permite realizar el seguimiento y avance.

?	E	Nombre	Fecha Inicial planificada	Fecha final planificada	Puntos	Responsable	HHP	HHC
✓	☑	Actualizar el Plan de Comunicaciones en el que se establecen mecanismos de capacitación y sensibilización en seguridad, gobierno y transformación digital, plataformas de infraestructura y arquitectura empresarial.	12/Feb/2024 00:00:00	30/Abr/2024 23:59:00	1	Martha Lucia Sanchez Niño	0	105
✓	☑	Actualizar, valorar y clasificar los activos de información de cada una de las dependencias de la UGG.	30/Ene/2024 00:00:00	26/Abr/2024 23:59:00	1	John Jeferson Valbuena Camacho	0	32
✓	☑	Actualizar, valorar y clasificar los riesgos asociados a los activos de información de cada una de las dependencias de la UGG.	02/May/2024 00:00:00	30/Jul/2024 23:59:00	1	John Jeferson Valbuena Camacho	0	9
✓	☑	Campaña día de la TICS, en la que se presentan las herramientas de uso general y nuevas tecnologías para todos los funcionarios de la UGG.	12/Feb/2024 00:00:00	10/May/2024 23:59:00	1	Fabio Alberto Osorio Betancur	0	0
✓	☑	Definir los nuevos planes de tratamiento de riesgos de seguridad para los riesgos identificados.	01/Ago/2024 00:00:00	26/Sep/2024 23:59:00	1	John Jeferson Valbuena Camacho	0	5
✓	☑	Evaluar el nivel de madurez MSPI con respecto a la norma NTC/ISO 27001:2022.	30/Ene/2024 00:00:00	26/Abr/2024 23:59:00	1	Yerson Daniel Quintero Zipa	0	48
✓	☑	Identificar los procesos que se pueden incluir en la ampliación del alcance a la certificación del SGSI para la UGG.	30/Ene/2024 00:00:00	26/Abr/2024 23:59:00	1	Yerson Daniel Quintero Zipa	0	11
✓	☑	Realizar campañas de socialización para el uso y apropiación de herramientas tecnológicas (almacenamiento y correo electrónico) que tiene el ministerio para sus funcionarios.	01/Abr/2024 00:00:00	28/Jun/2024 23:59:00	1	Cristhian Camilo Contreras Rodriguez	0	30
✓	☑	Recopilar las estrategias del Plan de Continuidad Tecnológico diseñadas por cada una de las entidades sectoriales del Ministerio de Defensa Nacional.	02/Jul/2024 00:00:00	26/Sep/2024 23:59:00	1	John Jeferson Valbuena Camacho	0	8
✓	☑	Reestructurar el DRP con sus servicios críticos hacia una estrategia CLOUD: Definir la matriz de roles y responsabilidades del recurso humano requerido para la implementación y operación de la estrategia DRP de los servicios críticos mediante el CAF en la UGG.	02/Sep/2024 00:00:00	28/Nov/2024 23:59:00	1	Carlos Alberto Alvarez Bermudez	0	0
✓	☑	Reestructurar el DRP con sus servicios críticos hacia una estrategia CLOUD: Estimar los costos para la implementación de la estrategia DRP de los servicios críticos en la UGG.	03/Jul/2024 00:00:00	29/Ago/2024 23:59:00	1	JORGE ALEXANDER GARZÓN MARTINEZ	0	0
✓	☑	Reestructurar el DRP con sus servicios críticos hacia una estrategia CLOUD: Rediseñar la estrategia DRP de servicios críticos en la UGG.	30/Ene/2024 00:00:00	26/Abr/2024 23:59:00	1	Sergio Andres Loaiza Avila	0	0
✓	☑	Revisión y corrección de las pruebas piloto que se realizaron en la vigencia 2023 a la implementación del protocolo de IPV6 de la entidad.	02/Jul/2024 00:00:00	26/Sep/2024 23:59:00	1	Luis Felipe Martinez Gutierrez	0	0
✓	☑	Sensibilizar al personal de la UGG en la detección y reporte de posibles incidentes cibernéticos, así como en ciberseguridad y ciberdefensa. CSIRT.	30/Ene/2024 00:00:00	26/Abr/2024 23:59:00	1	Sebastian Eduardo Montanez Marquez	0	15

Ilustración 5. Cumplimiento Implementación Política Seguridad Digital vigencia 2024 de la Unidad de Gestión General del Ministerio de Defensa Nacional
Fuente: elaboración propia MinDefensa

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

Como se aprecia en la ilustración 5, durante la vigencia 2024 las tareas que se propusieron para la implementación de la política de Seguridad Digital fueron cumplidas en su totalidad, con una puntuación del 100%.

3.3. DISEÑO Y FORMULACIÓN

Específicamente, en los temas de seguridad de la información se cuenta con la meta "Implementar el 100% de los controles priorizados en la declaración de aplicabilidad para fortalecer la seguridad de la información". La cual destaca a la seguridad como parte fundamental y transversal del negocio, por esta razón es necesario generar gobierno, lineamientos y acciones que permitan a la entidad mantener segura y disponible su información.

Por lo anterior, y teniendo en cuenta que en todo el mundo los ataques cibernéticos se han incrementado con métodos innovadores (Colombia no ha sido la excepción), las áreas de seguridad se están vinculando a la Estrategia de TI para aumentar la capacidad del Estado de enfrentar las amenazas cibernéticas; pues en el momento presenta grandes debilidades, pese a que existen iniciativas gubernamentales, privadas y de la sociedad civil que buscan contrarrestar sus efectos, no hay una coordinación interinstitucional apropiada. Por esta razón, la seguridad es parte fundamental y transversal del negocio, y es necesario apropiar los lineamientos, emitidos por el gobierno nacional, que permitan a la entidad mantener segura y disponible su información. Así, el uso y la estrategia de tecnologías de información conlleva a la necesidad y obligación de mejorar las herramientas de seguridad informática.

3.3.1. Metodología utilizada

Teniendo en cuenta que el Plan Estratégico de Seguridad y Privacidad de la Información constituye la base y apoyo en la implementación del Sistema de Gestión de Seguridad de la Información y de la Política de Seguridad Digital (incluida en los planes de MIPG), la metodología utilizada se basa en los formatos de autodiagnóstico establecidos por MinTIC y en el análisis GAP del SGSI con respecto a la norma ISO 27001:2013. De igual manera se soporta en los siguientes documentos:

- Modelo de Seguridad y Privacidad de la Información de MinTIC (MSPI - 2024).
- GAP NTC/ISO 27001:2013.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

- Evaluación FURAG

3.3.2. Planeación

A partir de los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI (2024) y la implementación del Sistema de Gestión de Seguridad de la Información (SGSI); se toma como base el ciclo de mejoramiento continuo PHVA, procurando que el SGSI del ministerio se revise de forma continua y se ajuste a las dinámicas y los cambios en la infraestructura y los procesos de la Entidad.

3.4. APROBACIÓN

3.4.1. Aprobación

El presente documento cuenta con la aprobación del Comité de Gestión y Desempeño Institucional, en representación de la Alta Dirección de la Unidad de Gestión General del Ministerio de Defensa Nacional para el SGSI, entendiendo que el objetivo de este plan Estratégico de Seguridad y Privacidad de la Información es identificar los controles necesarios para implementar las opciones de tratamiento de riesgos de seguridad de la información escogidas en el plan de tratamiento de riesgos, identificar cuáles son aplicables y cuáles no para el sistema de gestión, explicar los motivos de esa decisión, describir los objetivos que se lograrán con los controles y la forma de implementación.

3.4.2. Vigencia

El presente documento entra en vigor a partir de la fecha de su publicación y hasta el 31 diciembre del 2025, y deberá ser revisado al menos una vez al año y cada vez que en la Unidad de Gestión General del Ministerio de Defensa Nacional de Colombia sea impactado por cambios organizacionales o de infraestructura tecnológica, nuevas regulaciones o leyes aplicables.

La revisión y aprobación del Plan Estratégico de Seguridad de la Información se realizará anualmente.

La Unidad de Gestión General del Ministerio de Defensa Nacional se reserva el derecho de alterar o modificar partes de este documento, a fin de atender los requerimientos de su Sistema de Gestión de Seguridad de la Información (SGSI), así como los requisitos específicos, cuando sea necesario.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

DEFINICIONES

Acción correctiva: [NTC-ISO/IEC 27001] Acción tomada para eliminar la causa de una no conformidad asociada con los requisitos del Sistema de Gestión de Seguridad de la Información para prevenir que ocurran nuevamente.

Acción preventiva: [NTC-ISO/IEC 27001] Acción para eliminar la causa de una no conformidad potencial asociada con los requisitos del Sistema de Gestión de Seguridad de la Información para evitar que ocurran.

Activo de información: [basado en ISO 13335] Todo aquel elemento en que se procesa almacena o transmite información y que tiene un valor para la Entidad. Ej. bases de datos, programas de computación, plataforma tecnológica (procesamiento de datos, comunicaciones o seguridad informática), documentos impresos, recursos humanos, entre otros.

Administración de accesos: [Glosario ITIL v3] Es el proceso responsable de autorizar a los usuarios el uso de servicios de TI, información u otros activos. La administración de acceso ayuda a proteger la confidencialidad, integridad y disponibilidad asegurando que solo los usuarios autorizados pueden acceder o modificar los activos. La administración de accesos corresponde a las labores de creación, modificación, consulta, bloqueo, desbloqueo y eliminación de cuenta de un usuario.

Alta dirección: [Definición interna del Ministerio de Defensa Nacional] Conformada por el ministro de Defensa Nacional, los viceministros de Defensa y el secretario general.

Análisis de riesgos: [NTC-ISO/IEC 27002] Uso sistemático de la información para identificar fuentes y estimar riesgos.

Auditoría al sistema de gestión de seguridad de la información: [NTC ISO 19011] Examen sistemático e independiente para determinar si las actividades y los resultados relacionados con la seguridad de la información cumplen disposiciones preestablecidas, y si estas disposiciones se aplican en forma efectiva y son aptas para alcanzar los objetivos.

BCP (Business Continuity Plan): El Plan de Continuidad del Negocio es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre. El BCP incluye un plan de recuperación tras desastre para manejar interrupciones de TI. El objetivo es evitar interrupciones en los servicios de misión crítica y

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

restablecer la función completa de la organización de la forma más rápida y sencilla posible. Fuente: https://es.wikipedia.org/wiki/Plan_de_continuidad_del_negocio.

CAF: [https://www.caf.com/es/paises/colombia/quienes-somos/]. Es el banco de desarrollo de América Latina y el Caribe, en línea con la nueva orientación estratégica de país, plasmada en el Plan Nacional de Desarrollo 2022-2026 Colombia, potencia mundial de la vida. Y si bien nos unen retos en común a la región, Colombia demanda estrategias y enfoques diferenciados. Ese es el sentido de la nueva Estrategia País: acompañarlos en un crecimiento más inclusivo territorial.

Comité de gestión y desempeño institucional - CGDI: [Definición interna del Ministerio de Defensa Nacional] Es el máximo ente rector de los procesos de gestión en la Unidad de Gestión General, así como del sistema de gestión de seguridad de la información, y conformado por representantes de la alta dirección.

Confidencialidad: [NTC-ISO/IEC 27001] Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Continuidad de negocio: [Prácticas profesionales DRII] Proceso de gestión que busca permitir a una organización continuar con la operación de sus procesos bajo condiciones adversas.

Dirección de Tecnologías de la Información y las Comunicaciones - TICS: [Definición interna del Ministerio de Defensa Nacional] Dependencia de la Unidad de Gestión General del Ministerio de Defensa Nacional cuyas funciones y responsabilidades se indican en el Decreto 1874 del 30 de diciembre de 2021.

Disponibilidad: [NTC-ISO/IEC 27001] Propiedad que determina que la información sea accesible y utilizable a solicitud de una entidad autorizada.

DRP (Disaster Recovery Plan): [NTC-ISO/IEC 27001] Describe la secuencia de actividades que se tendrán que llevar a cabo para restablecer la operación normal de los servicios de TI que dan soporte a los servicios de negocio.

GAP: El análisis GAP ISO 27001 es una evaluación indispensable para las organizaciones que buscan seguridad y protección para sus activos de información, sean estos digitales, en papel o en otro medio. Con precisión, el análisis GAP ISO 27001 evalúa los controles de seguridad existentes, los procesos y los procedimientos implementados para garantizar la seguridad de la información, y los compara con los requisitos de la norma, para establecer qué es lo que falta para llegar a la conformidad.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

Gestión de TI: Es una práctica, que permite operar, innovar, administrar, desarrollar y usar apropiadamente las tecnologías de la información (TI). A través de la gestión de TI, se opera e implementa todo lo definido por el gobierno de TI. La gestión de TI permite a una organización optimizar los recursos, mejorar los procesos de negocio y de comunicación y aplicar las mejores prácticas. Fuente: https://www.aec.es/web/guest/centro- conocimiento/gestión-tic

Gestión del riesgo: [NTC-ISO/IEC 27001] actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

GRC (Gobierno, Riesgo y Cumplimiento)**:** Son las siglas de gobernanza, riesgo y cumplimiento, y se refiere a una estrategia que combina estos tres elementos para mantener una organización segura y en funcionamiento.

Incidente de seguridad de la información: [NTC-ISO/IEC 27001] Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: [NTC-ISO/IEC 27001] Propiedad de salvaguardar la exactitud y estado completo de los activos de información.

IPV6 (Internet Protocol Version 6): es la última versión del protocolo de Internet (IP) desarrollada por el Internet Engineering Task Force (IETF). Esta versión sustituye la versión 4 (IPv4) que se usaba hasta ahora y establece un procedimiento estándar para transmitir paquetes de datos en redes de computadores.

Log: [Definición interna del Ministerio de Defensa Nacional] Registro oficial de eventos durante un periodo de tiempo definido. En seguridad de la información un log es usado para registrar datos de las actividades y eventos ocurridos para un dispositivo o aplicación.

MSPI: Modelo de Seguridad y Privacidad de la Información - MSPI, está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la entidad, con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos. Fuente: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/.

Partes interesadas: [Definición interna del Ministerio de Defensa Nacional] Son aquellos individuos que influyen en el proceso de gestión de la seguridad de la información o son influenciados por él. Dentro del contexto del Sistema de Gestión de Seguridad de la Información

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

pueden considerarse como partes interesadas los usuarios internos, los clientes, los proveedores, la gerencia, etc.

Personal: [Definición interna del Ministerio de Defensa Nacional] funcionarios, contratistas internos o externos, pasantes y demás terceros de la Unidad de Gestión General.

PESI: El plan estratégico de seguridad de la información determina los objetivos a cumplir para salvaguardar la información en sus pilares de confidencialidad, integridad y disponibilidad. Fuente: https://www.mintic.gov.co/arquitecturati/630/articles- 9483_recurso_pdf.pdf

PETI: Plan Estratégico de TI, de acuerdo con el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI del Estado colombiano, el Plan Estratégico de las Tecnologías de la Información y Comunicaciones, es el artefacto que se utiliza para expresar la Estrategia de TI. El PETI hace parte integral de la estrategia de la institución y es el resultado de un adecuado ejercicio de planeación estratégica de TI. Fuente: https://www.mintic.gov.co/arquitecturati/630/articles-15031_recurso_pdf.pdf

Plataforma tecnológica: [Definición interna del Ministerio de Defensa Nacional] Equipos servidores, estaciones de trabajo, equipos activos de red y sistemas de información.

Propietario de la información: [NTC-ISO/IEC 27002] Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

PTR: El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización; adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital. Fuente: https://www.mintic.gov.co/portal/715/articles-135830_plan_tratamiento_seguridad_2020_u20200902.pdf.pdf

Registro: [NTC-ISO/IEC 27001] Documento que suministra evidencia objetiva de las actividades efectuadas o de los resultados alcanzados.

Riesgo: [NTC-ISO/IEC 27001] Combinación de la probabilidad de un evento y sus consecuencias.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

Sanitización: [Definición interna del Ministerio de Defensa Nacional] Proceso por el cual los equipos informáticos son evaluados y acondicionados para cumplir con los requisitos de seguridad de información antes de ser conectados a la red de la Entidad. También se considera parte de la sanitización, el proceso por el cual la información de un equipo informático es removida por completo, empleando mecanismos de borrado seguro al finalizar el contrato en el que está siendo utilizado, cuando finaliza su vida útil o cuando es asignado a un usuario diferente.

Servicios de procesamiento de información: [NTC-ISO/IEC 27002] Cualquier sistema de procesamiento de información, servicio, plataforma tecnológica o instalación física que los contenga.
Sistema de Gestión de Seguridad de la Información (SGSI): [NTC-ISO/IEC 27001] Conjunto de la estructura organizacional, procedimientos, procesos y recursos, basado en un enfoque de riesgo del negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Tercero o contratista: [Definición interna del Ministerio de Defensa Nacional] 1). Proveedor de un producto o servicio que afecta la calidad del servicio prestado por la Unidad de Gestión General, ya sea como persona natural o jurídica. 2). Personal que pertenece a las empresas que proveen un producto o servicio. 3). Personas que prestan sus servicios a la UGG en modalidad de pasantías.

UGG: [Definición interna del Ministerio de Defensa Nacional] Unidad de Gestión General.

FIRMA: ***Original debidamente firmado reposa en archivo de la Dirección Tecnologías de la Información y las Comunicaciones TICS***
ELABORÓ: MARTHA LUCÍA SÁNCHEZ NIÑO
CARGO: Coordinadora Grupo Seguridad Digital

FIRMA: ***Original debidamente firmado reposa en archivo de la Dirección Tecnologías de la Información y las Comunicaciones TICS***
APROBÓ: MAURICIO ANDRÉS TELLEZ GARCES
CARGO: Director (E) de Tecnologías de la Información y las Comunicaciones TICS

ANEXO: Cronograma DP-F-026 PESI 2025

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial