Plan de Seguridad y Privacidad de la Información

MINISTERIO DE DEFENSA NACIONAL

UNIDAD DE GESTIÓN GENERAL

2020

CONTROL Y APROBACION DEL DOCUMENTO

Versión:	02
Fecha de versión:	16/01/2020
Creado Por:	Área de Seguridad Informática
Aprobado Por:	Oficina Asesora de Sistemas
Nivel de Clasificación:	Restringido

Histórico de Cambios

Fecha	Versión	Creado por	Descripción del Cambio
20-01-2019	01	Área de Seguridad informática	Creación
16-01-2019	02	Área de Seguridad informática	Actualización

TABLA DE CONTENIDO

1. OBJETIVO 4
2. ALCANCE 4
3. NORMATIVA 4
4. MANUAL DE SEGURIDAD DE LA INFORMACION DE LA OAS 5
5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN 6
6. OBJETIVOS ESPECIFICOS DE LA POLITICA DE SEGURIDAD DE LA INFORMACION 6
7. ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACION 6
7.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN 6
7.2. REPRESENTANTE DE LA ALTA DIRECCIÓN DEL SGSI 7
7.3. LÍDER DE SEGURIDAD DE LA INFORMACIÓN 8
7.4. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN 9
7.5. GESTOR INTERNO DE SEGURIDAD DE LA INFORMACIÓN 9
9. ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2020 10
10. DIVULGACION DEL PLAN 10

1. OBJETIVO

Establecer las actividades que se planean realizar durante el año 2019 con el fin de continuar la mejora en la seguridad de la información.

2. ALCANCE

Las actividades del plan se circunscriben a las políticas del Sistema de Gestión de Seguridad de la información de la Oficina Asesora de Sistemas de la Unidad de Gestión General del Ministerio de Defensa Nacional.

3. NORMATIVA

- **Ley 1341 de 2009.** Por medio de la cual se definen los conceptos y principios relativos a la sociedad de la información y otros aspectos relacionados con las Tecnologías de la Información y las Comunicaciones; se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

- **Ley 1581 de 2012.** "Por la cual se dictan disposiciones generales para la protección de datos personales."

- **Decreto 1747 de 2000.** Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con: "Las entidades de certificación, los certificados y las firmas digitales".

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

- **Decreto 2573 de 2014.** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

- **Decreto 1078 de 2015**. Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y las comunicaciones – Título 9 – Capítulo I.

- **Decreto 415 de 2016**. Por el cual se adiciona el Decreto Único Reglamentario del Sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

- **Decreto 1499 de 2017**. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto único Reglamentario del sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley

1753 de 2015" define en su ARTÍCULO 2.2.22.3.2, "El Modelo Integrado de Planeación y Gestión, versión dos, como un marco de referencia que permite, dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos", en términos de calidad e integridad del servicio, con el fin de que se entreguen resultados que atiendan y resuelvan las necesidades y problemas de los grupos de valor. Este Modelo incluye las Políticas de Gobierno Digital y Seguridad Digital.

- **Decreto 1008 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 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, se determina el marco general para la formulación de las políticas públicas que regirán el sector de las TIC.

- **Resolución 1374 de 2012**. Por la cual se adiciona la resolución 127 de 2012 "Por la cual se crean y organizan Grupos Internos de Trabajo del Ministerio de Defensa Nacional".

- **Resolución 10584 de 2014.** Por la cual se modifica parcialmente la Resolución No.1374 del 14 de marzo de 2012. Por la cual se ajustan las funciones del Grupo de Tecnología de Información y las Comunicaciones.

- **Resolución 4859 de 2018,** Ministerio de Defensa Nacional, "Por el 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".

- **Resolución 5563 de 2018,** Ministerio de Defensa Nacional, "Por el cual se formula el "Plan Estratégico de Tecnologías de la Información y las Comunicaciones del Sector Defensa y Seguridad 2018-2022".

- **CONPES 3854 DE 2016**. Política Nacional de Seguridad Digital.

4. MANUAL DE SEGURIDAD DE LA INFORMACION DE LA OAS

El Objetivo del Manual de Seguridad de la Información para todos los usuarios internos, como funcionarios, contratistas, pasantes, y demás personas naturales o jurídicas que tengan a su cargo o hagan uso de cualquier activo de información de la Oficina Asesora de Sistemas de la Unidad de Gestión General del Ministerio de Defensa Nacional de Colombia.

El Alcance del Manual de Seguridad de la Información incluye las políticas del Sistema de Gestión de Seguridad de la Información para la Oficina Asesora de Sistemas de la Unidad de Gestión General del Ministerio de Defensa Nacional, a fin de garantizar la calidad, oportunidad y seguridad de la información.

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Oficina Asesora de Sistemas en cumplimiento con las funciones encomendadas por la Directiva Permanente Ministerial DIR2014-18, en su literal 3.2.2, se compromete a salvaguardar sus activos de información, protegiéndola mediante la pertinente gestión de riesgos, promoviendo una cultura de seguridad de la información, el cumplimiento de la normatividad vigente, requisitos legales, generando una oportuna gestión a los incidentes y aplicando mejores prácticas de forma continua y estratégicamente aplicadas a través de controles de seguridad, garantizar la confidencialidad, integridad y disponibilidad de la información y los activos que la resguardan.

6. OBJETIVOS ESPECIFICOS DE LA POLITICA DE SEGURIDAD DE LA INFORMACION

1. Crear en la Oficina Asesora de Sistemas una cultura de seguridad de la información a través de campañas de sensibilización dirigidas al personal que labora en esta dependencia.
2. Identificar los riesgos asociados a los activos de la información en la Oficina Asesora de Sistemas.
3. Gestionar el nivel aceptable del riesgo en los activos de la información en la Oficina Asesora de Sistemas.
4. Tratar efectivamente los incidentes de seguridad con el fin de identificar causas y realizar las acciones de corrección para la mejora continua del Sistema de Gestión de Seguridad de la Información.

7. ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACION

La estructura de seguridad de la información en la Oficina Asesora de Sistemas estará conformada por los siguientes actores o roles: Ref.: ISO/IEC 27001:2013 CL A.6.1.1.

7.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

a. Debe existir un Comité de Seguridad de la Información permanente y estable para el mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

b. El Comité de Seguridad de la Información tendrá las siguientes características:
   1) Es el máximo ente rector que regula todos los aspectos relacionados con la seguridad de la información en la Oficina Asesora de Sistemas de la Unidad de Gestión General del Ministerio de Defensa Nacional.
   2) Estará presidido por el Líder del área de Seguridad Informática de la Oficina Asesora de Sistemas.
   3) Este Comité estará integrado por un representante de la Jefatura de la Oficina Asesora de Sistemas, Líder del Área de Seguridad Informática, Líder del Área de Proyectos, el Oficial de Seguridad de la Información y Gestor interno de calidad y seguridad.
   4) A las sesiones del comité podrán invitarse, en el evento que así lo requieran, funcionarios públicos o particulares expertos en temas específicos, quienes podrán aportar sus conceptos y/o orientaciones requeridos.

c. Entre las funciones del Comité de Seguridad de la Información están:

1) Liderar y definir las actividades tendientes al fortalecimiento y mejora continua del Sistema de Gestión de Seguridad de la Información ante la alta dirección que permitan fortalecer la Seguridad de la Información de la Oficina Asesora de Sistemas del MDN.
2) Apoyar a los responsables del Grupo de Talento Humano, en las actividades de divulgación y realización de concienciación a los funcionarios sobre Seguridad de la Información.
3) Supervisar la gestión desarrollada por el líder del área de Seguridad de la Información en la dirección del Sistema de Gestión de la Seguridad de la Información de la Oficina Asesora de Sistemas del MDN.
4) Estudiar y conceptuar sobre los casos especiales de Seguridad de la Información que se presenten y afecten la Oficina Asesora de Sistemas del MDN, para recomendar las acciones pertinentes y apoyar la toma de decisiones.
5) Aprobar y revisar los objetivos y estrategias del Sistema de Gestión de la Seguridad de la Información.
6) Emprender las revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.
7) Avalar los planes de pruebas y análisis de vulnerabilidades externas e internas a los componentes de la plataforma tecnológica, con el fin de garantizar un alto nivel de seguridad y que se cuente con las herramientas adecuadas para la protección de la misma.
8) Validar y aprobar los riesgos residuales de seguridad de la información, el plan de tratamiento de riesgos y, la declaración de aplicabilidad propuesta por el Líder del área de Seguridad Informática de la Oficina Asesora de Sistemas.
9) Aprobar el estándar para realizar el levantamiento del inventario de activos de información, la clasificación y la rotulación de los mismos, de acuerdo con su nivel de confidencialidad y criticidad.
10) Desarrollar un plan estratégico para determinar el enfoque integral con el que se abordará la continuidad de las actividades del Sistema de Gestión de Seguridad de la Información de la Oficina Asesora de Sistemas.
11) Aprobar la metodología para el análisis de riesgos, donde se identifiquen los activos de información críticos, su impacto, las amenazas, vulnerabilidades y probabilidad de ocurrencia, y se establezcan las respuestas necesarias para su tratamiento.
12) Aprobar el Modelo de Gestión de Incidentes de Seguridad de la Información y tener conocimiento sobre los resultados de las investigaciones sobre los incidentes de Seguridad de la Información.
13) Evaluar las infracciones al Sistema de Gestión de Seguridad de la Información en la Oficina Asesora de Sistemas para aprobar acciones preventivas, correctivas o de mejora.
14) Mantener actualizada las políticas y procedimientos del Sistema de Gestión de Seguridad de la Información de acuerdo a la estrategia sectorial del Ministerio de Defensa Nacional.
15) Garantizar que se realicen auditorías internas del SGSI a intervalos planificados y conocer los resultados.
16) Darse su propio reglamento y demás que se determinen para él.

7.2. Representante de la Alta Dirección del SGSI

a. Será el responsable ante la Alta Dirección de asegurar que el Sistema de Gestión de Seguridad de la Información se establezca, implemente y mantenga de acuerdo con los requisitos de la norma internacional ISO 27001:2013 en la Oficina Asesora de Sistemas.

b. Entre las funciones del Representante de la Alta Dirección se encuentran:
   1) Ser el canal de comunicación entre la Alta Dirección, las gerencias y todas las áreas involucradas en el SGSI.
   2) Hacer seguimiento e informar a la Alta Dirección sobre el desempeño del SGSI.
   3) Validar la implementación y operación del SGSI.
   4) Facilitar y promover el desarrollo de iniciativas sobre seguridad de la información.

5) Conocer y validar la implementación de programas de formación y toma de conciencia relacionados con el SGSI.
6) Conocer los procedimientos de seguimiento y revisión del SGSI.
7) Conocer la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.
8) Conocer la revisión de las valoraciones de los riesgos a intervalos planificados, y el nivel de riesgo residual y riesgo aceptable identificado.
9) Conocer la realización de auditorías internas al SGSI.
10) Conocer las revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.
11) Validar la documentación del SGSI, desarrollada por el Líder de Seguridad de la Información.

7.3. Líder de Seguridad de la Información

a. Será el responsable ante la Oficina Asesora de Sistemas por la definición, implementación, operación, mantenimiento y mejoramiento del SGSI.

b. Entre las funciones del Líder de Seguridad de la Información se encuentran:
   1) Ejecutar las tareas de Seguridad de la Información que le asigne el Comité de Seguridad de la información de la Oficina Asesora de Sistemas.
   2) Mantener informado al Comité de Seguridad de la Información de la Oficina Asesora de Sistemas, sobre los eventos e incidentes de seguridad que se presenten al interior de la misma.
   3) Gestionar la implementación, operación y mejora del Sistema de Gestión Seguridad de la Información para la Oficina Asesora de Sistemas.
   4) Monitorear y evaluar nueva legislación y nuevas regulaciones para definir lineamientos a considerar en cuanto a la seguridad de información y aspectos relacionados con la privacidad de la información.
   5) Identificar los requisitos estatutarios, reglamentarios y contractuales pertinentes a seguridad de la información para el SGSI.
   6) Hacer conocer al Comité de Seguridad de la Información las responsabilidades legales de la Alta Dirección, también como su exposición bajo las leyes y regulaciones vigentes.
   7) Definir la estrategia de gestión de activos de información, coordinar su implementación y centralizar el monitoreo sobre su ejecución.
   8) Definir la estrategia de gestión de los riesgos de Seguridad de la Información, coordinar su implementación y centralizar el monitoreo sobre su ejecución.
   9) Hacer seguimiento, revisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información de la Oficina Asesora de Sistemas.
   10) Definir, documentar, mantener, divulgar y actualizar los procedimientos propios de la gestión del Sistema de Gestión de Seguridad de la Información.
   11) Supervisar el cumplimiento de los procedimientos del Sistema de Gestión de Seguridad de la Información.
   12) Promover la creación y actualización de las políticas y estándares de Seguridad de la Información y velar por el cumplimiento de las mismas.
   13) Apoyar la consolidación de la cultura de Seguridad de la Información entre todo el personal de la Oficina Asesora de Sistemas.
   14) Coordinar la difusión de cualquier comunicación relacionada con el Grupo de Seguridad de la Información.
   15) Participar activamente en las actividades convocadas por el Comité de Seguridad de la Información.
   16) Coordinar la realización periódica de auditorías internas y pruebas de vulnerabilidad de acuerdo con las políticas establecidas, previa autorización del Comité de Seguridad de la Información.
   17) Elaborar y proponer al Comité de Seguridad de la Información, planes, procedimientos y controles para el mejoramiento del Sistema de Gestión de Seguridad de la Información de la entidad.

18) Proponer al Comité de Seguridad de la Información, planes de capacitación y entrenamiento para difundir las políticas, normas y estándares de seguridad de la información al personal de la Oficina Asesora de Sistemas.
19) Definir y proponer el Modelo de Gestión de Incidentes de Seguridad de la Información, y revisarlo para detectar y establecer mejoramientos.
20) Apoyar y coordinar el desarrollo de actividades de investigación y búsqueda de información referente a Seguridad de la Información.
21) Elaborar los informes que le sean requeridos por el Comité de Seguridad de la Información sobre el Sistema de Gestión de Seguridad de la Información de la Oficina Asesora de Sistemas.
22) Coordinar la implementación de acciones preventivas y correctivas del Sistema de Gestión de Seguridad de la Información con los respectivos responsables, de acuerdo con los resultados de las auditorías internas o externas.
23) Implementar y hacer seguimiento al plan de mejora continua del Sistema de Gestión de Seguridad de la Información.
24) Liderar el proceso de certificación y recertificación, cuando la Oficina Asesora de Sistemas defina este propósito.
25) Proponer y apoyar proyectos de Seguridad de la Información para la Oficina Asesora de Sistemas.

7.4. Oficial de Seguridad de la Información

a. Este rol es apoyo para el Líder de Seguridad de la Información en la implementación de las actividades y controles necesarios para llevar a cabo la implementación del Sistema de Gestión de Seguridad de la Información.

b. Entre sus funciones se consideran las siguientes:
   1) Difundir la cultura de Seguridad de la Información entre todos los miembros de la Oficina Asesora de Sistemas y velar por la difusión y cumplimiento de las políticas y estándares de Seguridad de la Información.
   2) Asesorar y recomendar a las dependencias y dueños de procesos en temas relacionados con la protección de los activos de información.
   3) Apoyar al Líder de Seguridad de la Información en la implementación técnica y operativa de controles de seguridad de la información pertinentes al proceso de Seguridad de la Información.
   4) Participar en los procedimientos de autorizaciones que sean pertinentes para garantizar la protección de los activos de información de la Oficina Asesora de Sistemas.
   5) Apoyar a la Oficina Asesora de Sistemas en la definición de los controles que deberán contener los sistemas de información para garantizar la seguridad de la información y la mitigación de riesgos asociados.
   6) Liderar el Equipo de Respuesta de Incidentes para la gestión de incidentes de seguridad y consolidar los resultados del manejo de incidentes del SGSI.
   7) Participar activamente en el Comité de Seguridad de la Información.
   8) Apoyar al Líder de Seguridad de la Información durante la ejecución de las auditorías internas o externas al Sistema de Gestión de Seguridad de la Información.
   9) Reemplazar en sus funciones al Líder de Seguridad de la Información durante su ausencia.

7.5. Gestor Interno de Seguridad de la Información

a. Este rol es apoyo para el Líder de Seguridad de la Información y cumple con las mismas funciones definidas como Gestor Interno de Calidad, pero aplicable al Sistema de Gestión de Seguridad de la Información.

9. ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2020

Para la vigencia 2020 se tienen planificadas las siguientes actividades.

Actividad (Compromiso Gerencial)	Responsable	Fecha Inicial Planificada	Fecha Final Planificada	Observaciones
Estudio de factibilidad para la integracion basada en un gobierno SOA y el Bus de servicios Empresariales (EBS) que permita la publicacion y el consumo de los servicios de interoperabilidad de la UGG **RIESGO**	Líder Área de Sistemas de Información	1-feb-20	30-dic-20	Contratación
Diseño e implementación de inteligencia de negocios	Líder Área de Sistemas de Información	1-feb-20	30-dic-20	Contratación
Modelo para fortalecer y mantener los controles de seguridad en las aplicaciones sectoriales de SIATH y Nómina. **ANTICORRUPCIÓN**	Líder Área de Seguridad Informática	1-feb-20	30-dic-20	Contratación
Prestación de servicio integral de Seguridad Informática y de la Información orientados al análisis de vulnerabilidades de plataformas críticas, pruebas de penetración e ingeniería social a través de pruebas prestablecidas.	Oficial de Seguridad de la Información OAS	1-jun-20	30-dic-20	Contratación
Campañas de sensibilización de Seguridad de la Información para colaboradores de la OAS.	Oficial de Seguridad de la Información OAS	1-ene-20	31-dic-20	Una cada trimestre con recursos propios

10. DIVULGACION DEL PLAN

El procedimiento de comunicaciones del plan de Seguridad y Privacidad de la Información debe estar acorde con los lineamientos internos del MINISTERIO DE DEFENSA NACIONAL – UGG en materia de comunicaciones internas y externas.

Se identifican dos grandes grupos de Interesados: internos y externos.

1. Clientes internos: Servidores públicos y contratistas de la UGG – OAS.

   Internamente se realizará la divulgación del PETI como componente de la Política de Gobierno Digital, en conjunto con las otras Políticas de Gestión y Desempeño contenidas en el Modelo Integrado de Planeación y Gestión.

2. Clientes externos: Organismos de Control, Ministerio de las TIC y Ministerio de Defensa.