CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de los cambios
1	Diciembre 2020	Versión Inicial. Elaboración por primera vez del documento.

CONTROL DE APROBACIÓN

Aprobó:	CR. Luis Hernando Sandoval Pinzón Subdirector Técnico y de Gestión de DIGSA	
Revisó:	CS. Vivian Tatiana Alba Díaz Gestor de Calidad PROGTIC	CR. Carlos Darío González Villamil Coordinador Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA
	SMSM. Edna del Pilar Martínez Páez Grupo Planeación Estratégica DIGSA Líder Área Sistemas Integrados de Gestión ARSIG	PD. Alexandra Martínez Vargas Coordinadora Grupo Planeación Estratégica DIGSA Representante de la Dirección
Elaboró:	PD. Yolanda Quintero Agudelo Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA Área Seguridad de la Información DIGSA	PD. Diana Marcela López Bejarano Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA Área Seguridad de la Información DIGSA

1. Presentación

Este procedimiento surge de la necesidad de crear y documentar las políticas de seguridad de información, como parte integral del Sistema de Gestión de Seguridad de la Información, enmarcados dentro del Modelo de Seguridad y Privacidad de la Información - MSPI.

2. Objetivo

Definir las actividades y controles para gestionar las políticas de Seguridad de la Información de la Dirección General de Sanidad Militar – DIGSA, de acuerdo a las necesidades de la Entidad, directrices y lineamientos del Comando General de las Fuerzas Militares, del Ministerio de Defensa Nacional y del Ministerio de Tecnologías de la Información y de las Comunicaciones, así como a la normatividad legal vigente.

3. Alcance

Aplica a toda la organización y en especial a los funcionarios, contratistas, proveedores y terceras partes relacionados que tengan acceso, disponibilidad u operación con los activos de información, los servicios digitales y/o sistemas de información de la Dirección General de Sanidad Militar - DIGSA, así como aquellos usuarios que son responsables o tienen custodia sobre los activos de información de la Entidad.

4. Políticas de Operación

Información:	4.1	Las políticas de Seguridad de la Información definidas por la DIGSA se deben comunicar a los funcionarios y/o contratistas, así como a las demás partes interesadas de la Entidad, de manera que sean accesibles, de fácil comprensión y pertinentes a los requisitos de la misma.
	4.2	Las políticas adoptadas por la DIGSA, salvaguardan las características de confidencialidad, disponibilidad e integridad de la información, las cuales están definidas conforme a los objetivos estratégicos y los requisitos normativos colombianos vigentes.
	4.3	Es necesario el liderazgo y compromiso de la alta Dirección, además de la participación activa de los funcionarios, contratistas y partes interesadas para dar cumplimiento a los lineamientos, requisitos y buenas prácticas de seguridad de la información, así como el desarrollo de estrategias de mejora continua y la gestión oportuna ante incidentes o eventos de seguridad de la información.
	4.4.	El Oficial de Seguridad de la Información o quien haga sus veces es responsable de coordinar con el área encargada de las comunicaciones institucionales, las campañas de socialización de las políticas para asegurar que todos los funcionarios, contratistas y/o partes interesadas de la DIGSA, las conozcan, se comprometan con su cumplimiento y sean conscientes de las sanciones que puede acarrear el no cumplimiento de las mismas.

	4.5	Las políticas establecidas en el marco seguridad de la información deben estar sujetas a una revisión anual o en el evento de cambios estructurales que afecten a la Entidad.

5. Definiciones

Política:	Declaración, intenciones y directrices de la organización, expresadas por la alta dirección.
Seguridad de la información:	Preservación de la confidencialidad, integridad y disponibilidad de la información.
Sistema de Gestión de Seguridad de la Información (SGSI):	Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una entidad para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.
Oficial de Seguridad de la información:	Es la persona responsable de planear, coordinar y administrar los procesos de seguridad informática en una organización.
Políticas de Seguridad Informática:	Son las directrices de índole técnica y de organización que se llevan adelante respecto de un determinado sistema de computación a fin de proteger y resguardar su funcionamiento y la información en él contenida.
Seguridad:	Asegurar que los recursos del sistema de información (material informático o programas) o portales de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

6. Acrónimos

DIGSA:	Dirección General de Sanidad Militar.
SISAM	Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones
SGSI:	Sistema de Gestión de Seguridad de la Información.
MSPI	Modelo de Seguridad y Privacidad de la Información.
NTC:	Norma Técnica Colombiana.
ISO:	International Organization for Standarization
AREIN:	Área de Seguridad de la Información
ARECO:	Área de Infraestructura Tecnológica, Redes y Comunicaciones
ARIBD:	Área administración del Sistema y Base de Datos

7. Proveedor – entrada (insumo) para el desarrollo del procedimiento

Proveedor	Entrada - insumo
Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).	El Modelo de Seguridad y Privacidad de la Información (MSPI).
COMPES 3854	Política de Seguridad Digital del Estado Colombiano
Ministerio de Defensa Nacional	Directiva Permanente 018 de 2014
Comando General de las FFMM	Directiva Permanente 154 de 2014
Dirección General de Sanidad Militar	Políticas y lineamientos sobre seguridad de la información emitidos mediante Resoluciones y Circulares en la Entidad.

8. Descripción de Actividades y Puntos de Control

Descripción	Registro(s)
1. Definir las políticas de seguridad de la información dando cumplimiento a las leyes, reglamentos pertinentes (Anexo A. de la NTC ISO/IEC 27001:2013) y los requisitos de la Entidad. En el caso de la DIGSA, incluye los requisitos dados por el Ministerio de Tecnologías de Información y las Comunicaciones – MINTIC, a través, del Modelo de Seguridad y Privacidad de la Información – MSPI. Responsable: Alta Dirección de la DIGSA Subdirector Técnico y de Gestión o quien haga sus veces, Coordinador del Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones (Ver punto de control).	Documento con las Políticas del Sistema de Gestión de Seguridad de la Información
2. Aprobar las políticas de seguridad de la información. Responsable: Alta Dirección de la DIGSA Subdirector Técnico y de Gestión o quien haga sus veces. Coordinador del Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones	Actas, Manuales, Resoluciones con respecto de las Políticas del Sistema de Gestión de Seguridad de la Información aprobadas.
3. Comunicar y socializar las políticas de seguridad de la información a los funcionarios y partes interesadas, por medio de programas de inducción, re-inducción, sensibilización y capacitación. Responsable: Coordinador Grupo Sistema Integral de Información –	Registros de capacitaciones (Documentación, soportes fotográficos, entre otros.)

Descripción	Registro(s)
Tecnologías de la Información y la Comunicaciones - AREIN	
4. Publicar en el sistema de información designado por la Entidad, la versión final y aprobada de las políticas de Seguridad de la Información, que se consideren pertinentes publicar, sin que se revele información reservada de la DIGSA. Responsable: Coordinador Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones - AREIN Coordinador Grupo Planeación Estratégica	Página Web, Correo electrónico institucional, entre otros medios digitales.
5. Mantener actualizado el manual del SGSI y las políticas de seguridad de la información cuando los cambios en la entidad lo exijan. Además, se debe realizar una revisión anual de actualización; estos cambios pueden estar relacionados con: - Estructura organizacional. - Condiciones del entorno. - Infraestructura interna. - Condiciones legales. - Ambiente técnico Responsable: Líder de Seguridad de la Información o delegado. Coordinador Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones.	Manual del sistema de gestión de seguridad de la información (SGSI) Políticas del Sistema de Gestión de Seguridad de la Información
6. Generar una cultura de seguridad de la información en los funcionarios, proveedores y partes interesadas de la DIGSA para dar a conocer y difundir las políticas correspondientes. Responsable: Líder de Seguridad de la Información o delegado. Coordinador Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones. (ver punto de control).	Registros de capacitaciones (Documentación, soportes fotográficos, entre otros.)
7. Diseñar, definir y realizar un programa de auditoría para el Sistema de Gestión de Seguridad de la Información de la entidad- SGSI, en el cual se contemplen los diferentes dominios de seguridad y las políticas asociadas. Responsable: Área de Sistemas integrados de Gestión o Control Interno. Coordinador Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones.	Programa de auditoria por parte del área de sistemas integrados de gestión. Auditoria por parte de los entes de control (Min TIC)

Descripción	Registro(s)
Fin.	

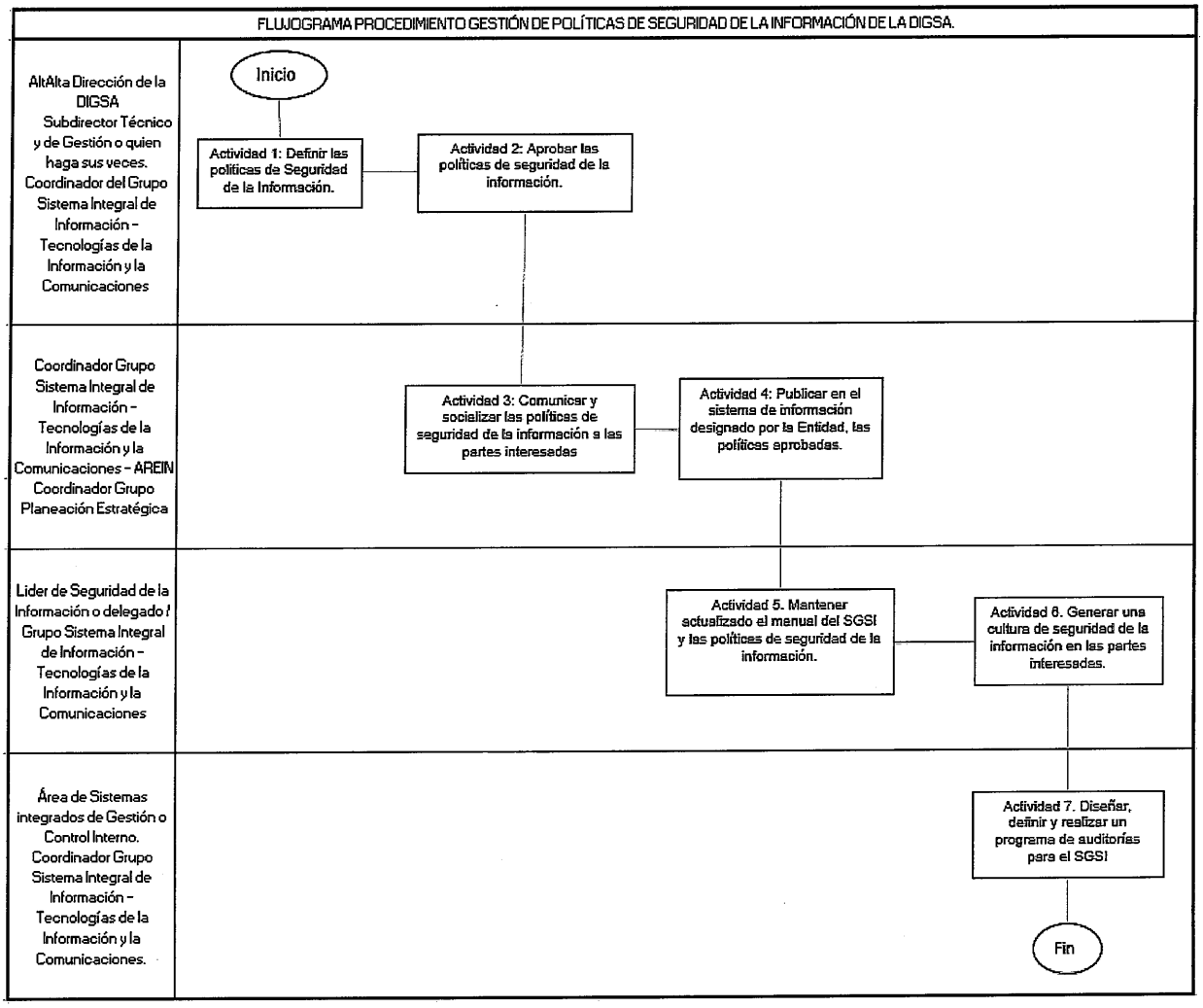
Puntos de control

Actividad donde se controla:	1. Definir las políticas de seguridad de la información dando cumplimiento a las leyes, reglamentos pertinentes (Anexo A. de la NTC ISO/IEC 27001:2013) y los requisitos de la Entidad. En el caso de la DIGSA, incluye los requisitos dados por el Ministerio de Tecnologías de Información y las Comunicaciones – MINTIC, a través, del Modelo de Seguridad y Privacidad de la Información – MSPI.
Como se controla:	Observando el documento con las Políticas del Sistema de Gestión de Seguridad de la Información
Criterio de aceptación	Si no están definidas las políticas de seguridad de la información dando cumplimiento a las leyes, reglamentos pertinentes (Anexo A. de la NTC ISO/IEC 27001:2013) y los requisitos de la Entidad (DIGSA).
Acción a tomar (si no cumple criterio de aceptación):	Devolver el documento al dueño del proceso por correo electrónico especificando las observaciones de incumplimiento.
Registro de la acción tomada:	Correo electrónico enviado.
Responsable del control:	Alta Dirección de la DIGSA. Coordinador del Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones

Puntos de control

Actividad donde se controla:	6. Generar una cultura de seguridad de la información en los funcionarios, proveedores y partes interesadas de la DIGSA para dar a conocer y difundir las políticas correspondientes.
Como se controla:	Observando los Registros de capacitaciones (documentación, soportes fotográficos, entre otros.)
Criterio de aceptación	Si no hay registros de capacitaciones (documentación, soportes fotográficos, entre otros), de la DIGSA.
Acción a tomar (si no cumple criterio de aceptación):	Generar correo electrónico al responsable del proceso, especificando observaciones de incumplimiento.
Registro de la acción tomada:	Correo electrónico enviado.
Responsable del control:	Líder de Seguridad de la Información o delegado. Coordinador Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones.

9. Flujograma



10. Documentos y registros relacionados

10.1. Manual del Sistema de Gestión de Seguridad de la Información
10.2. Políticas y Procedimientos de Seguridad de la Información de DIGSA.
10.3. NORMA ISO/IEC 27001:2013. Anexo A (Normativo). A. 5.
10.4. Modelo de seguridad y privacidad de la información- MSPI
10.5. Políticas de seguridad de la información para las Fuerzas Militares