

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA
"General Rafael Reyes Prieto"



Resolución Número **41** de 2024

11 JUL 2024

"Por la cual se definen los roles y responsabilidades de seguridad de la información en la Escuela Superior de Guerra "General Rafael Reyes Prieto""

EL DIRECTOR DE LA ESCUELA SUPERIOR DE GUERRA
En uso de sus atribuciones legales y estatutarias

CONSIDERANDO:

Que a través del decreto 1008 del 14 de junio 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".

Que el Decreto 1008 de 2018, subroga las disposiciones en materia de la Estrategia de Gobierno en Línea por la "Política de Gobierno Digital".

Que mediante Resolución 7870 de 2022 del Ministerio de Defensa Nacional "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".

Que la Escuela Superior de Guerra "General Rafael Reyes Prieto" "ESDEG", mediante Resolución No. 025 del 02 de mayo de 2023, por medio de la cual se fortalece el Comité Institucional de Gestión y Desempeño, se ajusta su reglamento de funcionamiento, se asignan roles y responsabilidades para el Sistema Integrado de Gestión SIG-ESDEG, y se establecen los procesos que lideran las dimensiones del Modelo Integrado de Planeación y Gestión.

Que la ESDEG, mediante Acta No. 01241312-MDN-COGFM-JEMCO-ESDEG-DIESG-PLAES del 11 de julio de 2024 de Reunión de Comité Institucional de Gestión y Desempeño, aprobó la Política Institucional de seguridad digital y de la información ESDEG.

Que la ESDEG, mediante Acta No. 01241312-MDN-COGFM-JEMCO-ESDEG-DIESG-PLAES del 11 de julio de 2024 en Reunión de Comité Institucional de Gestión y Desempeño, aprobó los Roles y Responsabilidades de Seguridad de la Información.

RESUELVE:

ARTÍCULO 1º. Objeto. Adoptar los requisitos para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información "SGSI" alineados con la ISO/IEC 27001:2013, ISO/IEC 27001:2022 y ISO-IEC 27002:2022, implementando las políticas institucionales relacionadas con la seguridad de la Información y los datos.

ARTÍCULO 2º. Ámbito de Aplicación: El SGSI de la ESDEG, abarca y aplica a todos los procesos de la entidad, por consiguiente, todos los funcionarios militares y civiles, estudiantes, docentes, prestadores de servicio y demás partes interesadas que debido al cumplimiento de sus funciones o actividades compartan, utilicen, recolecten, procesen, intercambien o consulten información, quienes deberán realizar los esfuerzos requeridos para su cumplimiento.

ARTÍCULO 3º. Roles y responsabilidades del Sistema de Gestión de Seguridad de la Información "SGSI": Para el SGSI al interior de la ESDEG, se definirán los siguientes roles y responsabilidades:

1. Subdirección.

- a) Responder por la asignación de recursos y designación de responsabilidades para la gestión de la seguridad de la información al interior de la ESDEG.
- b) Gestionar el nombramiento del oficial de Seguridad de la Información en la ESDEG.

2. Comité de Seguridad de la Información.

Las funciones del comité de Seguridad de la Información son asumidas por el Comité Institucional de Gestión y Desempeño, así:

- a) Asegurar la implementación del SGSI y las políticas institucionales relacionadas con la seguridad de la Información y los datos al interior de la ESDEG.
- b) Revisar los diagnósticos del estado de la seguridad de la información en la ESDEG.
- c) Acompañar e impulsar el desarrollo de proyectos de seguridad de la información en la ESDEG.
- d) Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la ESDEG.
- e) Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
- f) Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- g) Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
- h) Promover la difusión y sensibilización de la seguridad de la información dentro de la ESDEG.

Parágrafo Primero. El Comité podrá invitar con voz y sin voto, al Oficial de Seguridad de la Información a las sesiones de Comité, en las cuales se trata temas de seguridad y privacidad de la información.

3. Jefe DETIC (Oficial líder de Tecnologías de la Información y Comunicaciones)

- a) Coordinar la implementación del Sistema de Gestión de Seguridad de la Información en la ESDEG.
- b) Liderar el desarrollo de los planes, programas y proyectos de tecnologías de información y las comunicaciones de la ESDEG de acuerdo con los lineamientos y objetivos para el

fortalecimiento institucional establecidos por el Sector Defensa en cabeza del Comando General de las Fuerzas Militares.

- c) Responder porque las estrategias de seguridad de la información de la ESDEG estén alineadas con las tecnologías de la información para lograr los objetivos planificados.
- d) Analizar y realizar propuestas para mejorar los procesos de las tecnologías de la información de la entidad.
- e) Planear el costo en infraestructura de tecnologías de la información y comunicaciones.
- f) Establecer mejoras e innovaciones de soluciones a los requerimientos de tecnologías de información y las comunicaciones de la ESDEG.
- g) Diseñar, asesorar, impulsar y poner en marcha las estrategias para la debida implementación y mejoramiento continuo de la gestión estratégica de las tecnologías de información y las comunicaciones que contribuyen al logro de los objetivos misionales de la ESDEG bajo las directrices y orientaciones del Comando General de las Fuerzas Militares.

4. Oficial de Seguridad de la información

- a) Responder por la implementación de las Políticas de Seguridad de la información que van siendo aprobadas por el Comité de Gestión y Desempeño de la ESDEG.
- b) Definir, actualizar y difundir las políticas, procedimientos y formatos del SGSI.
- c) Supervisar, evaluar o verificar la administración del control de acceso a la información.
- d) Responder por la seguridad y privacidad de los datos en la ESDEG.
- e) Definir los planes de entrenamiento y sensibilización en lo referente a seguridad de la información.
- f) Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de la implantación de las medidas de seguridad de la información.
- g) Gestionar los riesgos asociados a la seguridad de los activos de información de la ESDEG.
- h) Liderar el equipo de respuesta ante los incidentes de seguridad de la información en la ESDEG.
- i) Supervisar el cumplimiento normativo de la seguridad de la información.

5. Dueños de proceso

- a) Identificar e inventariar los activos digitales de información y los riesgos asociados.
- b) Verificar los informes de auditorías realizadas a la seguridad digital y responder porque se apliquen las acciones correctivas identificadas, así como las recomendaciones entregadas por los auditores.
- c) Realizar el análisis de riesgos de seguridad de la información de sus procesos y coordinar el plan de tratamiento con el Oficial líder de Tecnologías.
- d) Acudir, permitir y exigir la asistencia de sus funcionarios a las capacitaciones programadas en cuanto las políticas, procedimientos y formatos del SGSI.


6. Usuarios, que son todos los funcionarios militares y civiles, estudiantes, docentes, prestadores de servicio y demás partes interesadas:

- a) Cumplir con las políticas de seguridad y privacidad de la Información de la ESDEG.
- b) Aplicar los principios de confidencialidad, disponibilidad e integridad de la información que produzcan, conozcan o transmitan dentro y/o afuera de la entidad y aquella que sea relativa a la misionalidad de la entidad y que se encuentre dentro del entorno laboral como también dentro del entorno personal y de las redes sociales.
- c) Reportar incidentes de seguridad al oficial de Seguridad de la información.
- d) Participar activamente en las campañas de sensibilización y capacitación en SGSI.

ARTÍCULO 4º. Control Interno. El Control Interno es asumido por la Inspección General de las Fuerzas Militares. De acuerdo con la Resolución No. 25 del 02 de mayo de 2023 ESDEG, en el Artículo 17 º. "Líneas de Defensa SIG ESDEG. De las cuatro líneas de defensa del esquema de responsabilidades establecido en la 7a Dimensión "Control Interno" del Modelo Integrado de Planeación y Gestión MIPG, en el SIG ESDEG se implementan la Línea de Defensa Estratégica, la 1a y 2a Línea de Defensa, toda vez, que la 3a Línea de Defensa está bajo la responsabilidad de la Inspección General de las Fuerzas Militares, por ser la competente funcional y legal para asumir las responsabilidades de una unidad u oficina de control interno."

ARTICULO 5 º. Vigencia: La presente resolución rige a partir de la fecha de su expedición y publicación.

COMUNÍQUESE Y CÚMPLASE.



Brigadier General Jaime Alonso Galindo
Director Escuela Superior de Guerra "General Rafael Reyes Prieto"

2023

2048


Vo Bo: Contralmirante Omar Yesid Moreno Oliveros
Subdirector Escuela Superior de Guerra

Revisó:



VIADM: CR. Verónica Pedraza Martínez
Jefe Vicedirección Administrativa


PLAES: MY. Adriana Marcela Vargas Aguilar
Jefe Planeación Estratégica ESDEG (E)


JURID: CT. María Paola Castillo Calderón
Jefe Oficina Jurídica ESDEG

Estructuró:


DETIC: MY. David Leonardo Núñez Capacho
Jefe Departamento TIC


DETIC: PD6. Blanca Inés Santana Rodríguez
Ingeniero de Sistemas DETIC