Nombre de la Política	Fecha Aprobación (dd/mm/aa)	Proceso-Dependencia Responsable de la Política
POLITICA INSTITUCIONAL DE SEGURIDAD DIGITAL Y DE LA INFORMACION	11/07/2024	A04 Gestión TIC

POLÍTICA

La Escuela Superior de Guerra "General Rafael Reyes Prieto" ESDEG, para el cumplimiento de su misión institucional busca proteger la confidencialidad, integridad y disponibilidad de los activos de información; mediante la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), estableciendo un marco de confianza hacia los grupos de valor y partes interesadas.

OBJETIVO (s) DE LA POLÍTICA

1. Proteger los activos de información de la ESDEG.
2. Fortalecer la continuidad de los servicios de TI y mitigar los riegos asociados al servicio.
3. Fortalecer la cultura de seguridad de la información en la comunidad académica ESDEG.
4. Mitigar el impacto de los incidentes de seguridad y privacidad de la información en la ESDEG.

MARCO CONCEPTUAL DE LA POLÍTICA

1. Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de está (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
2. Activo de información: es todo aquello que tiene algún valor para la organización y que por ende, debe protegerse. (ISO 27001).
3. Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
4. Comité de seguridad de la Información. Es quien debe asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo. Si no existe este Comité, las funciones de este comité serán asumidas por el Comité Institucional de Gestión y Desempeño.
5. Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 27000).
6. Cultura Organizacional. Es la sensibilización y capacitaciones a las partes interesadas para generar conciencia en el uso y aprovechamiento de las tecnologías de la información y comunicaciones para garantizar la confidencialidad, integridad y disponibilidad de la información.
7. DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (ISO/IEC 27000).

8. Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
9. Identificación y clasificación de activos de información: Consiste en generar un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios.
10. Incidente de seguridad de la información: Es cualquier evento que tenga el potencial de afectar la preservación de la confidencialidad, integridad y disponibilidad o valor de la información.
11. Integridad: Propiedad de la información relativa a su exactitud y completitud. (ISO/IEC 27000).
12. Manual de políticas de seguridad y privacidad de la información: Abarca las Políticas Generales en Seguridad de la Información, alineados la norma ISO 27001 de 2013/2022 (se establecen los controles de buenas prácticas en seguridad de la información).
13. MSPI : Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad. Da las pautas para que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.
14. Partes interesadas: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. (MSPI- Ministerio de Tecnologías de la Información y Comunicaciones).
15. Plan de continuidad del negocio. Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
16. Procedimientos y formatos de seguridad de la información: Consiste en desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad.
17. Gestión de incidentes de seguridad y privacidad de la información: Es establecer las actividades para dar cumplimiento con el ciclo de vida de la gestión y respuesta a un incidente de seguridad. Estas actividades son a) detección y análisis, b) contención, erradicación y recuperación y c) actividades posts-incidentes.
18. Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
19. Roles y Responsabilidades. Consiste en definir los roles y responsabilidades para la implementación del Modelo de Seguridad y Privacidad de la Información- MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados como manuales, procedimientos, formatos, etc.
20. Seguridad de la información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información. Además, otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas. (ISO/IEC 27000).
21. Sistema de gestión de seguridad de la información: Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos de información que se manejan dentro de una entidad.
22. Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o mas amenazas. (ISO/IEC 27000).

FUNDAMENTO LEGAL DE LA POLÍTICA

1. Constitución Política de Colombia. Artículos 15, 20, 23 y 74.
2. Ley 1581 del 17 de octubre de 2012. "Por la cual se dictan disposiciones generales para la protección de datos personales".
3. Ley 1712 del 06 de marzo de 2014. "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
4. Decreto 1078 de 2015 del 26 de mayo de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
5. Decreto No. 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" A partir de este Decreto se cambia el modelo anterior de la Estrategia de Gobierno en Línea, para dar paso a la Política de Gobierno Digital.
6. Resolución 500 de 10 de marzo de 2021 "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".
7. Resolución 7870 del 26 de diciembre 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.
8. Resolución 448 del 14 de febrero de 2022 "Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se deroga la Resolución 2256 de 2020".
9. Normas ISO/IEC 27001:2013, ISO/IEC 27001:2022 y ISO-IEC 27002:2022.

ALCANCE DE LA POLÍTICA

Grupos de Valor / Cliente, Grupos de Interés / Partes Interesadas, Procesos del Sistema Integrado de Gestión ESDEG, Servicios de Educación Superior, en general a toda la comunidad académica ESDEG.

ÁMBITOS DE APLICACIÓN DE LA POLÍTICA

La presente política se desarrolla a través del ciclo PHVA, así:

PLANEAR

1. DETIC: Revisar y/o actualizar la resolución de roles y responsabilidades de la seguridad de la información cuando sea pertinente.
2. DETIC: Realizar diagnóstico de seguridad y privacidad de la información en la ESDEG.
3. DETIC: Definir lineamientos para el levantamiento de activos de información.
4. DETIC: Definir, publicar y socializar el procedimiento de incidentes de seguridad de la información cuando sea pertinente.

5. DETIC: Revisar o actualizar el manual de políticas de seguridad de la información cuando sea pertinente. Estas políticas basadas en los controles de la Norma ISO/IEC 27001:2022, como son controles organizacionales, controles de personas, controles físicos y controles tecnológicos.
6. DETIC: Revisar o actualizar el plan de continuidad del negocio cuando sea pertinente.

HACER:

7. DETIC: Presentar para aprobación del Comité Institucional de Gestión y Desempeño, el documento de roles y responsabilidades de seguridad de la información.
8. Procesos ESDEG: Realizar el levantamiento o actualización de los activos de información.
9. DETIC: Publicar los activos de información.
10. Procesos ESDEG: Actualizar los riesgos de seguridad de la información.
11. DETIC: Socializar el manual de políticas de seguridad de la información.
12. DETIC: Gestionar los incidentes y/o ataques de Seguridad de la Información identificados.
13. DETIC: Implementar el plan de continuidad del negocio.
14. DETIC: Presentar en el CIGD los riesgos o afectaciones a la seguridad de la información en la ESDEG, proponiendo los cursos de acción efectivos para mitigar la materialización del riesgo.
15. DETIC: Realizar campañas de sensibilización y capacitaciones a las partes interesadas para generar conciencia en el uso y aprovechamiento de las tecnologías de la información y comunicaciones para garantizar la confidencialidad, integridad y disponibilidad de la información.

VERIFICAR:

16. DETIC: Realizar seguimiento a los incidentes de seguridad de la información reportados a la mesa de servicio de acuerdo con lo establecido en el procedimiento definido.
17. VIADM: Realizar el seguimiento a los informes de eventos y vulnerabilidades de seguridad de la información.
18. Procesos ESDEG: Analizar, valorar y controlar los riesgos de seguridad de la información.
19. DETIC: Efectuar seguimiento al plan de continuidad del negocio.
20. PLAES: Realizar seguimiento a las acciones correctivas y oportunidades de mejora producto de revisiones internas y externas en materia de seguridad de la información.
21. DETIC: Verificar el uso y la aplicabilidad del manual de políticas de seguridad de la información.

ACTUAR:

22. PLAES: Determinar No conformidades a las que haya lugar.
23. PLAES: Formular e implementar acciones correctivas y oportunidades de mejora a las que haya lugar.
24. DETIC: Elaborar plan de mejoramiento y cargar las actividades en SVE.

INSTRUCCIONES RELACIONADAS CON LA POLÍTICA
1. Las Políticas Institucionales de Gestión se deben aprobar en el Comité Institucional de Gestión y Desempeño. 2. Las Políticas Institucionales Académicas se deben aprobar en Consejo Académico. 3. Los Dueños de proceso responsables de la política efectuarán el seguimiento y evaluación estratégica en el contexto de implementación de esta y de los ámbitos de aplicación, para proponer los ajustes que se consideren necesarios.

REVISÓ	VISTO BUENO	APROBÓ
MY. Adriana Marcela Vargas Aguilar Jefe Planeación Estratégica (E)	2024 CA. Omar Yesid Moreno Oliveros Subdirector ESDEG	2024 BG. Jaime Alonso Galindo Director ESDEG

ESTRUCTURÓ	VALIDÓ	REVISIÓN JURÍDICA	ACTO ADMINISTRATIVO VOLUNTAD INSTITUCIONAL SOBRE LA POLÍTICA
PD6. Blanca Inés Santana Rodríguez Ingeniero de sistemas DETIC MY. David Leonardo Núñez Capacho Dueño de Proceso / Jefe DETIC	CR. Verónica Pedraza Martínez Jefe Vicedirección Administrativa CR. (R) Mario Fernando Canales Rodríguez Asesor Planeación Estratégica	CT. Maria Paola Castillo Calderón Jefe Oficina Jurídica ESDEG	Acta No. 01241312- MDN-COGFM-JEMCO-ESDEG-DIESG-PLAES, de fecha 11/07/2024 Aprobación: Comité Institucional de Gestión y Desempeño