Nombre de la Política	Fecha Aprobación (dd/mm/aa)	Proceso-Dependencia Responsable de la Política
POLÍTICA INSTITUCIONAL DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN ESDEG	08/OCT/2018	A04 Gestión TIC

POLÍTICA
(Redacción concreta de la intención Institucional de la Política /qué/)

Fortalecer la seguridad y privacidad de la información en la Escuela Superior de Guerra a través de la implementación de los lineamientos de seguridad de todos los activos de información y la gestión de riesgos de seguridad digital, que contribuyan a incrementar la confianza de los grupos de valor y partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información de la entidad.

OBJETIVO (s) DE LA POLÍTICA
(Finalidad (es) de la política /para qué/))

1. Proteger los activos de información de la Escuela Superior de Guerra frente a amenazas internas y externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad, mediante la implementación de controles efectivos.
2. Generar mecanismos para que la Escuela Superior de Guerra pueda establecer los elementos para identificar, analizar, valorar y mitigar los riesgos, amenazas y vulnerabilidades del entorno digital
3. Mejorar la toma de decisiones por parte de la Escuela Superior de Guerra, Grupos de Valor y Partes interesadas a través del fortalecimiento la cultura de seguridad de la información mediante capacitaciones y sensibilizaciones.
4. Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la Escuela Superior de guerra para optimizar su articulación.

MARCO CONCEPTUAL DE LA POLÍTICA
(conceptos que fundamentan la política)

1. Definición de Roles y Responsabilidades. Consiste en asignar Roles y responsables para realizar las tareas o actividades encaminadas a la implementación seguridad digital y de información, y la gestión de riesgos.

2. Identificación y clasificación de Activos Informáticos: 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.

3. Activo Informático: Es un activo que contiene información pública que utiliza la organización para funcionar en el entorno digital Estos activos pueden ser aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información, tecnologías de operación.

4. Seguridad de la información

   a) Estado actual del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad.
      - Estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad.
      - nivel de madurez de los controles de seguridad y privacidad de la información en la entidad.
      - Nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
      - uso de buenas prácticas en ciberseguridad.
   b) Política de seguridad y privacidad de la información: consiste en elaborar el manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la ESDEG.
   c) Procedimientos 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.
   d) Integración del MSPI con el Sistema de Gestión documental: La ESDEG deberá alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el archivo general de la nación.
   e) Plan de transición de IPv4 a IPv6. Consiste en realizar la transición de IPv4 a IPv6 para Colombia que indica las actividades específicas a desarrollar.

5. Riesgos

   a) Diagnóstico de la entidad: Consiste en conocer la entidad en cuanto:
      - Misión, visión, objetivos estratégicos y planeación institucional.
      - Caracterización de los procesos, objetivos de los procesos, planes, programas o proyectos asociados.
   b) Identificar los riesgos inherentes de seguridad digital. Consiste en determinar las causas, con base en los factores internos, externos y del proceso analizados para la ESDEG y que pueden afectar el logro de los objetivos:

      Preguntas claves para la identificación de riesgos:
      - ¿Qué puede suceder? Permite identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.
      - ¿Cómo puede suceder? Permite establecer las causas a partir de los factores determinados en el contexto
      - ¿Cuándo puede suceder? Permite determinar de acuerdo al desarrollo del proceso
      - ¿Qué consecuencias tendría su materialización? Permite determinar los posibles efectos por la materialización del riesgo.

   c) Tipología de riesgos:
      - Riesgos estratégicos: posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
      - Riesgos gerenciales: posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección
      - Riesgos operativos: posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
      - Riesgos financieros: posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

- Riesgos tecnológicos: posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
- Riesgos de cumplimiento: posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
- Riesgo de imagen o reputacional: posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas
- Riesgos de corrupción: Posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Riesgos de seguridad digital: Posibilidad Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- Otras tipos de riesgos son: Crediticio, ambiental, de mercado, de liquidez, satisfacción del cliente, seguridad alimenticia, peligro para humanos.

d) Valoración de los riesgos: Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial. Elementos que lo desarrollan:

- Análisis de riesgos: Consiste en determinar la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).
- Evaluación de riesgos: Consiste en confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL).
- Tratamiento de riesgos: El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:
  - Aceptar el riesgo: Consiste en no adoptar ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado)
  - Evitar el riesgo: Consiste en abandonar las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.
  - Reducir el riesgo: Consiste en adoptar medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.
- Monitoreo de riesgos: Consiste en evaluar periódicamente los riesgos para determinar la efectividad de los planes de tratamiento y de los controles propuestos. Se tiene la matriz de responsabilidades.
- Seguimiento a los riesgos: Consiste en generar reportes periódicos del estado de los riesgos.

6. Cultura Organizacional. Consiste en definir un Plan de comunicación, sensibilización y capacitación a los grupos de valor y partes interesadas para apoyar a la eficiencia de los procesos SIG ESDEG y contribuir al logro de las metas y objetivos institucionales.

FUNDAMENTO LEGAL DE LA POLÍTICA

(Relación de las normas y lineamientos que sustentan la política, incluidas las propias de la ESDEG)

1. Ley 1581 de octubre 07 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales"

2. Ley 1712 de marzo 06 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".
3. Directiva Permanente No. DIR2014-18 de 2014. Políticas de Seguridad de la Información para el Sector Defensa
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. Modelo de Seguridad y Privacidad de la Información del Ministerios de las Tecnologías de la Información y las Comunicaciones (MINTIC).
6. Modelo de gestión de riesgos de seguridad digital (MGRSD) 2018.
7. Política de Operación Riesgos del 09 de mayo de 2018 Departamento Administrativo de la Función Pública.
8. Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas del agosto de 2018 del Departamento Administrativo de la Función Pública.

ALCANCE DE LA POLÍTICA
(Identifique a quien va dirigida y la cobertura de aplicación 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
(Identifique el Proceso, aspecto o función sustantiva de la educación y defina las estrategias necesarias para implementar la Política que asegure su articulación con el Planeamiento Estratégico de la ESDEG)

1. Definición de roles y responsabilidades

   a) Designar un responsable de seguridad de la Información que a su vez responderá por la seguridad digital en la entidad.
   b) Involucrar funcionarios de cada proceso para la identificación de los activos de TI en la ESDEG.

2. Identificación y clasificación de activos de información.

   a) Listar los activos TI por cada proceso en la ESDEG (indicando algún consecutivo, nombre y descripción breve de cada uno de los activos).
   b) Identificar el dueño o responsable de cada uno de los activos TI en la ESDEG.
   c) Clasificar los activos según su naturaleza (Información, Software, Hardware, Componentes de Red entre otros).
   d) Clasificar la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable.
   e) Determinar la criticidad del activo para su valoración (criticidad ALTA, MEDIA y BAJA).
   f) Identificar si existen infraestructuras críticas cibernéticas.

3. Política general de seguridad de la información.

   a) Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la ESDEG.

b) Determinar el nivel de madurez de seguridad y privacidad de la información en la ESDEG
c) Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
d) Identificar el uso de buenas prácticas en ciberseguridad en la ESDEG.
e) Elaborar el manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la ESDEG.
f) Desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la ESDEG,
g) Alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el archivo general de la nación.
h) Realizar el plan de transición de IPv4 a IPv6 para Colombia que indica las actividades específicas a desarrollar.

4. Riesgos TI.

a) Obtener un conocimiento de la ESDEG en cuanto a misión, visión, objetivos, procesos, planes, programas o proyectos.
b) Identificar o definir los riesgos de TI en la ESDEG
c) Clasificar los riesgos de TI en la ESDEG de acuerdo a la topología.
d) Describir los riesgos de acuerdo a la tipología, causas y consecuencias.
e) Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto.
f) Definir el tratamiento para cada uno de los riesgos analizados y evaluados.
g) Elaborar la matriz de responsabilidades para el monitoreo de los riesgos de TI en la ESDEG.
h) Realizar reportes periódicos para llevar el seguimiento de los riesgos de TI en la ESDEG.

5. Cultura organizacional en seguridad y privacidad de la información.

a) Realizar campañas de sensibilización en cuanta seguridad y privacidad de la información para minimizar la ocurrencia de incidentes de seguridad de la información.
b) Concientizar a los grupos de valor y partes interesadas de la ESDEG en el uso del entorno digital y del aseguramiento de los activos de información.
6. Elaborar plan de comunicación, sensibilización y capacitación para los usuarios académicos y administrativos de la ESDEG.

INSTRUCCIONES RELACIONADAS CON LA POLÍTICA
(Tenga en cuenta para tramitar y asegurar la implementación de la Política)

1. Para las iniciativas de Política Institucional de Gestión, debe observarse:

a) Formulación, por parte de la dependencia, proceso o responsable de la dimensión del Modelo Integrado de Planeación y Gestión MIPG.
b) Validación, a través de Planeación Estratégica.
c) Aprobación, a través del Comité Institucional de Gestión y Desempeño

2. En coherencia con los ámbitos de aplicación de la política, el proceso/dependencia responsable de la misma, debe proponer las acciones/actividades de implementación de la política, con una línea de tiempo hasta de cuatro años, identificando para cada vigencia las acciones/actividades a cumplir con los procesos/dependencias que deban estar comprometidos.

3. Las acciones/actividades de implementación de la política, quedarán registradas en los respectivos planes de acción y articulados con el planeamiento estratégico de la ESDEG.

4. Planeación Estratégica efectuará el seguimiento y evaluación estratégica en el contexto de implementación de la Política y de los ámbitos de aplicación, para proponer los ajustes que se consideren necesarios.

VISTO BUENO	REVISÓ	APROBÓ
~~CR. Raul Alonso Parra Bayona~~ Jefe Planeación Estratégica	BGCIM. Oscar Eduardo Hernández Duran Subdirector ESDEG	MG. Francisco Javier Cruz Ricci Director ESDEG

ESTRUCTURO	VALIDACIÓN PLANEACIÓN ESTRATÉGICA	REVISIÓN JURÍDICA	ACTO ADMINISTRATIVO VOLUNTAD INSTITUCIONAL SOBRE LA POLÍTICA
Mayor Elizabeth Bocarejo Bautista Dueño de Proceso Gestión TIC Jefe Departamento TIC	CR. (ra) Canales Rodriguez Mario Fernando Asesor Planeación Estratégica	TE. Andrea del Pilar Perez Guecha Jefe Jurídica	Acta No. 1435 -MDN-COGFM-JEMCO-ESDEG-PLAES-2.25, de fecha 08 de octubre de 2018 Aprobación: Comité Institucional de Gestión y Desempeño