PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EJERCITO NACIONAL DE COLOMBIA

Departamento de Comunicaciones (CEDE6)

2026

TABLA DE CONTENIDO

LISTA DE TABLAS

TABLA DE ILUSTRACIONES

1. INTRODUCCIÓN

El Ejército Nacional en el marco del Modelo Integrado de Planeación y Gestión (MIPG), específicamente en el desarrollo de las Políticas Gobierno Digital y Seguridad Digital, establece el presente Plan Estratégico de Seguridad y Privacidad de la Información, que se integra al plan de acción institucional, de conformidad con el Decreto 612 del 04 de abril de 20181.

Por consiguiente, este documento presenta el plan de trabajo a seguir en la vigencia 2026 para el desarrollo de las actividades orientadas a cumplir con los lineamientos y estándares de seguridad de la información de la Política Gobierno Digital dispuestos en el Decreto 767 del 16 de mayo de 20222, y los establecidos en la Política Seguridad Digital, de acuerdo con la Resolución 00500 de marzo 10 de 20213.

En atención a lo anterior, el Ejército Nacional pone en conocimiento de los grupos de interés y de la ciudadanía el Plan Estratégico de Seguridad y Privacidad de la Información para la vigencia 2026, mediante el cual se define un conjunto articulado de actividades estructuradas bajo el ciclo de mejora continua Planear, Hacer, Verificar y Actuar (PHVA), orientadas a consolidar condiciones de uso confiable y seguro de la información en los entornos digital y físico.

Dicho Plan adopta un enfoque basado en la gestión del riesgo, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información institucional, así como de establecer controles técnicos, administrativos y operacionales que permitan prevenir, mitigar y gestionar posibles afectaciones a los activos de información que soportan la ejecución, evaluación y continuidad de los procesos institucionales. Lo anterior, en concordancia con el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones, y con fundamento en los lineamientos establecidos en la Norma Técnica Colombiana NTC-ISO 27001:2022 "Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos".

---

1 Ejército Nacional, FO-CEDE5-DIPLE-1852, (2024,07 junio), Versión 1*"Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado".*

2 "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".

3 "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". Fortalecida por la Resolución 746 de 2022 y Resolución 2277 de 2025.

En virtud de estos parámetros, se busca fortalecer un entorno institucional de seguridad digital, confianza y transparencia en la gestión pública, asegurando que la implementación del modelo adoptado se traduzca en una solución eficaz y eficiente, que permita mantener y elevar los niveles de seguridad de la información requeridos al interior de la Institución, en cumplimiento de la misión constitucional y legal asignada al Ejército Nacional.

2. DEFINICIONES

Activo de información: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tenga valor para la organización[4]. (ISO/IEC 27001:2022).

Amenazas: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización[5]. (ISO/IEC 27001:2022).

Análisis de riesgo: proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo[6]. (ISO/IEC 27001:2022).

Auditoría: proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría.[7] (ISO/IEC 27001:2022).

Bases de datos personales: conjunto organizado de datos personales que sea objeto de Tratamiento.[8] (Ley 1581 de 2012, artículo 3°). Por la cual se dictan disposiciones generales para la protección de datos personales.

Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo[9].

---

[4] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5, 2025, pág. 8.
[5] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5, 2025, pág. 8
[6] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5, 2025, pág. 8

[7] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5, 2025, pág. 8.
[8] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5, 2025, pág. 8
[9] Función Pública, Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 7, pág. 55.

Confidencialidad: propiedad de la información que determina que esté disponible a personas autorizadas.[10].

Controles de seguridad en la información: son incluyen políticas, reglas, prácticas y estructuras organizativas que pueden ser de naturaleza administrativa, técnica, de gestión o legal, con el propósito de gestionar el riesgo y proteger la información de una organización.[11].

Ciberseguridad: protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentra interconectados.[12]

Ciberespacio: red interdependiente de infraestructuras de tecnología de la información que incluye internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados en industrias.[13] (Decreto 338 de 2022).

Disponibilidad: propiedad de la información de estar accesible y utilizable a demanda por una entidad[14].

Tratamiento de Datos personales: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.[15] (Ley 1581 de 2012, art 3).

Datos personales públicos: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y

---

[10]Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Glosario, https://www.mintic.gov.co/portal/inicio/Glosario/.

[11] *International Organization for Standardization. (2022).* ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. *ISO.*

[12] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, pág. 9.

[13] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, pág. 9.

[14] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Guía para la administración del Riesgo y el diseño de controles en entidades públicas versión 6. Pág. 15.

[15] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5, 2025 pág. 18.

sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva[16] (Decreto 1377 de 2013, art 3).

Bases de Datos personales: conjunto organizado de datos personales que sea objeto de tratamiento[17] (Ley 1581 de 2012, art 3).

Datos personales sensibles: se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales y/o de derechos humanos. Del mismo modo, se consideran datos sensibles aquellos que promuevan intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición. También clasifican en esta categoría, los datos relativos a la salud, a la vida sexual y los datos biométricos.[18] (Decreto 1377 de 2023, art 3, numeral 3).

Evaluación del riesgo: busca 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)[19].

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[20].(ISO/IEC 27001:2022).

Impacto estratégico: se refiere al efecto significativo que decisiones, acciones o iniciativas tienen sobre el rendimiento organizacional, incluyendo la capacidad de la empresa para alcanzar sus objetivos estratégicos, mejorar su competitividad y responder a cambios en su entorno interno y externo. Es una medida del efecto causal que una estrategia tiene sobre los resultados clave de la organización.[21]

Integridad de la información: es uno de los tres pilares fundamentales de la seguridad informática. Se refiere a la protección de los datos contra la alteración o

---

[16] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5, 2025 pág. 11.
[17] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5, 2025 pág. 11.
[18] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5, 2025 pág. 11.
[19] Función Pública, Guía para la Administración del Riesgo y el diseño de controles en entidades públicas.2022, versión 6. Pág. 61.
[20] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5, 2025 pág. 12.
[21] Pınar Başar, R. M. (2023). *Impact of Strategic Management on Competitive Advantage.* Trends in Business and Economics, 37(1), 46–56.

destrucción no autorizada, asegurando que la información sea precisa y consistente durante todo su ciclo de vida[22].

Probabilidad: posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.[23]

Plan de continuidad del negocio: Un plan de continuidad del negocio (o Business Continuity Plan, BCP) es un documento organizacional que contiene un conjunto predeterminado de instrucciones, procedimientos y estrategias para mantener o restaurar las funciones críticas de una empresa durante y después de una interrupción significativa, con el objetivo de minimizar impactos negativos y asegurar la operación continua de procesos esenciales.[24]

Privacidad de la información (o de datos): es el derecho y la capacidad de las personas para controlar la recopilación, uso, almacenamiento y divulgación de sus datos personales.[25]

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 27001:2022). [26]

Riesgo de seguridad digital: es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que puede afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.[27]

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO/IEC 27001:2022).[28]

Sistema de Gestión de Seguridad de la Información (SGSI): conjunto de elementos interrelacionados (estructura organizativa, políticas, planificación de

---

[22]HostDimeBlog, (2023, 22 agosto), Integridad de la información en seguridad informática. https://www.hostdime.la/blog/integridad-de-la-informacion-en-seguridad-informatica/

[23] Función Pública, Guía para la Administración del Riesgo y el diseño de controles en entidades públicas versión 6. Pág.13.

[24]. National Institute of Standards and Technology. (s. f.). *Business continuity plan (BCP)*. CSRC Glossary. Recuperado de https://csrc.nist.gov/glossary/term/business_continuity_plan

[25] International Organization for Standardization. (2011). *ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework*. ISO, 2011, Pág. 1.

[26] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5, 2025, Pág. 17

[27] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5, 2025, Pág.17

[28] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5, 2025, Pág. 18

actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.[29]

Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad[30]. (ISO/IEC 27000).

Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas.[31] (ISO/IEC 27000).

ESPACIO EN BLANCO DEJADO INTENCIONALMENTE

[29].Sistema Integrado de Gestión, Instructivo del sistema de Gestión de Seguridad de la Información, https://colaboracion.dnp.gov.co/CDT/DNP/SIG/Brochure%20SGSI%202021.PDF Pág. 1

[30] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5, 2025, Pág. 18.

[31] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5, 2025, Pág.19.

3. OBJETIVO

Establecer e implementar la estrategia institucional orientada a propender por el uso, la clasificación, la protección y el aseguramiento de los activos de información del Ejército Nacional, conforme a la normatividad vigente y a los lineamientos aplicables en materia de seguridad y privacidad de la información.

4. ALCANCE

El Ejército Nacional, en atención a la importancia estratégica de la adecuada gestión, protección y administración de la información institucional, asume el compromiso de implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI), como instrumento orientado a consolidar un marco de confianza institucional en el cumplimiento de sus funciones constitucionales y legales frente al Estado y la ciudadanía.

En ese sentido, con el propósito de fortalecer dicho marco de confianza, resulta indispensable la protección integral de los activos de información, mediante la adopción e implementación de controles técnicos, administrativos y operativos que permitan identificar, gestionar y mitigar de manera sistemática los riesgos, reduciendo su probabilidad de materialización y su impacto, y asegurando un nivel de exposición aceptable conforme a los lineamientos y normatividad vigente, preservando en todo momento los principios de confidencialidad, integridad y disponibilidad de la información.

En consecuencia, el Sistema de Gestión de Seguridad de la Información (SGSI) establece disposiciones y controles de obligatorio cumplimiento, aplicables a la totalidad de los procesos institucionales, funcionarios, contratistas, terceros, proveedores y demás partes interesadas que, en desarrollo de sus funciones o por razón de su interacción con la Institución, accedan, recolecten, utilicen, consulten, almacenen, transmitan, intercambien, procesen o administren información del Ejército Nacional.

5. CONTEXTO

El Sistema de Gestión de Seguridad de la Información (SGSI), se establece e implementa alineado con la misión del Ejército Nacional de Colombia en la cual se requiere "*Conducir operaciones militares orientadas a defender la soberanía, la independencia y la integridad territorial y proteger a la población civil y los recursos*

privados y estatales para contribuir a generar un ambiente de paz, seguridad y desarrollo, que garantice el orden constitucional de la nación"[32].

Por consiguiente, el **Sistema de Gestión de Seguridad de la Información (SGSI)** establece los lineamientos institucionales en materia de **seguridad y privacidad de la información**, orientados a garantizar la **integridad, disponibilidad y confidencialidad** de los activos de información del Ejército Nacional, en concordancia con la estructura documental y los parámetros definidos en el **Sistema Integrado de Gestión**.

En este sentido, el SGSI se articula con el **Sistema de Gestión de Calidad**, permitiendo atender de manera integral los requisitos normativos y de obligatorio cumplimiento, así como fortalecer los procesos internos, optimizar el uso de los recursos institucionales y consolidar capacidades estratégicas para la protección de la información.

Adicionalmente, el **Ejército Nacional de Colombia**, en su estructura organizacional, se encuentra integrado por **cuatro Jefaturas de Estado Mayor**, las cuales, en cumplimiento de los direccionamientos impartidos por el Gobierno Nacional, deberán adoptar y aplicar los lineamientos definidos en el **Sistema de Gestión de Seguridad de la Información (SGSI)**, para su implementación y sostenibilidad en el marco de sus competencias y responsabilidades funcionales.

ESPACIO EN BLANCO DEJADO INTENCIONALMENTE

[32] El Ejército Nacional de Colombia, (2025, 29 julio), página web https://www.ejercito.mil.co/mision-y-vision/ difunde la Misión institucional que se refiere a la conducción de las operaciones militares orientadas a defender la soberanía Colombiana.

Ilustración 1. Organigrama del Ejército Nacional de Colombia

***Fuente:** organización del Ejército Nacional de Colombia*

Con la finalidad de dar cumplimiento a la Directiva Permanente 2025228010640103 del 16 de junio de 2025, "Lineamientos para el desarrollo de la Política General de Seguridad de la Información en el Ejército Nacional", se han creado misionalidades particulares para las diferentes dependencias que se deberán desarrollar con el fin de avanzar en el desarrollo del sistema de gestión de seguridad de la información (SGSI).

Con el propósito de apoyar el desarrollo de las dimensiones de gestión con valores para resultados, establecidas en la Resolución 4240 de 15 de junio de 2018 del Ministerio de Defensa Nacional[33], para el cumplimiento de las políticas de gestión y desempeño institucional como son Gobierno Digital, Seguridad Digital, y transparencia, acceso a la información pública y lucha contra la corrupción, en el

[33] Por la cual se adopta el Modelo Integrado de Planeación y Gestión, se integra el Modelo Estándar de Control Interno en el Sector Defensa, se crea el Comité de Gestión y Desempeño para el Sector Defensa, el Comité de Coordinación del Sistema de Control Interno, el Comité Sectorial de Auditoría Interna, se establecen otros lineamientos y se derogan unas Resoluciones.

Plan Estratégico de la Información y las Comunicaciones del Sector Defensa y Seguridad (PETI 2022 -2026) define las directrices esenciales para la adecuada gestión de las Tecnologías de la Información y las Comunicaciones al interior de la Fuerza. En concordancia con lo anterior, el artículo 7, numeral 3, de la Resolución 4240 de 2018, relativo a los Planes de Acción Anuales, establece que las unidades ejecutoras y vinculadas al Ministerio de Defensa Nacional deben incluir, dentro de sus líneas de acción, los planes institucionales y estratégicos señalados en el artículo 1 del Decreto 612 de 2018 expedido por el Departamento Administrativo de la Función Pública. Entre dichos planes se encuentra el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI). En razón de lo anterior, el presente plan se modifica con el fin de alinearse con el Plan de Acción Institucional del Ejército Nacional y con el PETI del Ministerio de Defensa Nacional.

6. ALINEACIÓN ESTRATÉGICA SECTORIAL

El Plan Estratégico Institucional del Ejército Nacional "Hombres y Mujeres de Honor al servicio de la Nación 2022-2026" define dos enfoques transversales, cuatro perspectivas, cinco líneas estratégicas y diez objetivos estratégicos, fundamentales para alcanzar el estado final deseado a corto y mediano plano. Este conjunto de elementos, a través de la alineación estratégica, subraya la contribución del Ejército Nacional al cumplimiento de los objetivos del Sector Defensa y del Estado Colombiano.[34]

Considerando que para la formulación del Plan Estratégico Institucional se tuvo en cuenta la Constitución Política de la República de Colombia (CPC[35]), el Plan Nacional de Desarrollo 2022 – 2026" (PND[36]), Política de Seguridad, Defensa y Convivencia Ciudadana "Garantías para la Vida y la Paz 2022-2026, el Plan Estratégico Sectorial del Ministerio de Defensa Nacional,[37] el Plan Estratégico Institucional del Comando General de las Fuerzas Militares, el Plan Estratégico Militar de Transformación (PEMT2042[38]) y los Diálogos Regionales Vinculantes (DRV[39]) en relación con las necesidades de los grupos de valor; el Ejército Nacional realizó un ejercicio de analítica de datos que permitió identificar y acoger aquellos

[34] Plan Estratégico Institucional PEI 2022-2026 (2024, 15 noviembre), https://www.ejercito.mil.co/plan-estrategico-institucional-pei-2022-2026/

[35] Constitución Política de Colombia, (1991,20 julio), (https://www.policia.gov.co/sites/default/files/descargables/1.%20CONSTITUCION%20POLITICA%20DE%20COLOMBIA_0.pdf

[36] Colombia Potencia Mundial de la vida, (2022-2026), https://colaboracion.dnp.gov.co/CDT/Prensa/Publicaciones/plan-nacional-de-desarrollo-2022-2026-colombia-potencia-mundial-de-la-vida.pdf

[37] Plan Estratégico del Sector Defensa y Seguridad, Guía de Planeamiento Estratégico (2022-2026), https://www.casur.gov.co/wp-content/uploads/2025/10/PES2024_MDN.pdf

[38] Plan Estratégico de Transformación Ejército del Futuro 2042, (2023, 18 mayo), https://www.ejercito.mil.co/plan-estrategico-de-transformacion-ejercito-del-futuro-2042/

[39] Colombia Tienes La Palabra, Diálogos Regionales Vinculantes, (2025, 19 diciembre) https://dialogosregionales.dnp.gov.co/

elementos trascendentales que aportarán decididamente a la gran estrategia de los niveles superiores.

La alineación estratégica institucional 2022-2026 se articula entre las partes interesadas como se muestra en la siguiente gráfica expuesta a continuación en forma jerárquica de izquierda a derecha Estrategia Nacional, y continúa con Estrategia Sectorial, Estrategia Comando General y Estrategia del Ejército Nacional.

Ilustración 2 *Alineación Estratégica Ejército Nacional*

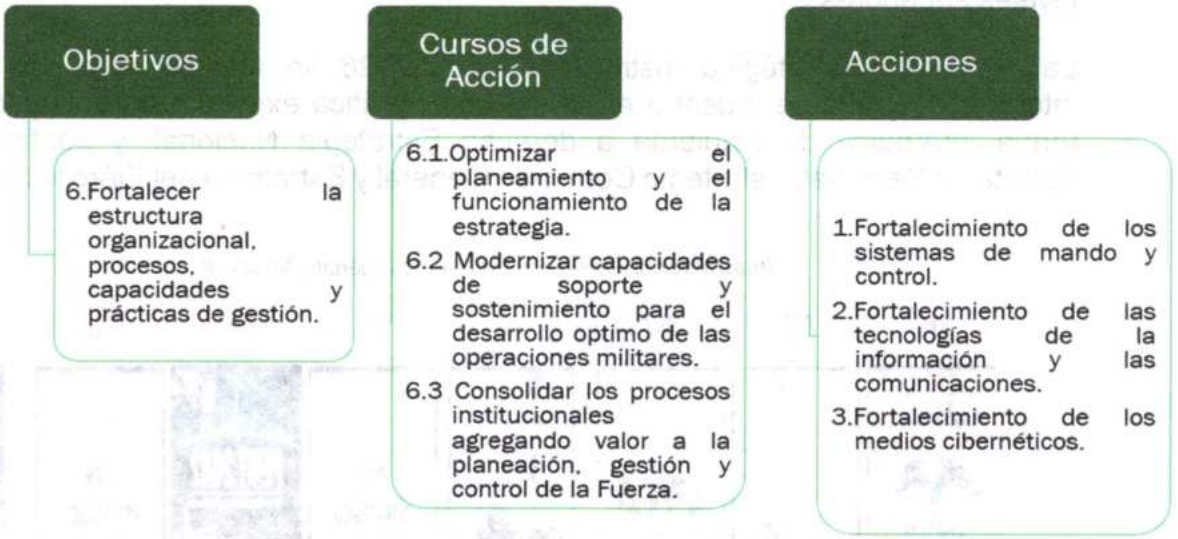
Fuente: *Guía de Orientación Estratégica Departamento de Planeación (CEDE5)*

En el marco del Plan Estratégico Institucional (PEI) 2022-2026, los objetivos estratégicos de Tecnologías de la Información (TI), están orientados al fortalecimiento de la infraestructura TIC institucional, contribuyen directamente al cumplimiento del objetivo estratégico del Ejército Nacional establecido en dicho Plan: **"6. Fortalecer la estructura organizacional, los procesos, las capacidades y las prácticas de gestión"**. Este objetivo se materializa a través de los cursos de acción definidos y del cumplimiento de las metas establecidas, así:

1. Optimizar el planeamiento y el funcionamiento de la estrategia.
2. Modernizar capacidades de soporte y sostenimiento para el desarrollo optimo de las operaciomes militares.
3. Consolidar los procesos institucionales agregando valor a la planeación, gestión y control de la Fuerza.

Es asi que a través del análisis de cada indicador, se evidencia el porcentaje de cumplimiento a las metas propuestas y el mejoramiento en la prestación de los servicios de Tecnologías de Información y Comunicaciones en el Ejército Nacional.

***Ilustración 3** Aportes TIC a la Estrategia*



***Fuente:** Plan Estratégico Institucional 2022-2026 (PEI)*

7. PREMISAS

El presente Plan responde a las necesidades institucionales de seguridad de la información, fortaleciendo la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), teniendo en cuenta lo siguiente:

7.1 Cumplir con los principios de seguridad de la información, lo cual significa propender por el cumplimiento de la confidencialidad, la integridad y la disponibilidad de la información.

7.2 El Plan cumple con los principios de la administración pública, definidos por el Departamento Administrativo de la Función Pública, por lo cual "está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones"[40].

7.3 El Ejército Nacional propende por el apoyo en la innovación tecnológica, la cual es fundamental en la toma de decisiones con respecto al Sistema de Gestión de Seguridad de la Información (SGSI).

[40] Constitución Política de Colombia, art. 209

7.4 El Sistema de Gestión de Seguridad de la Información (SGSI) emite las políticas, procedimientos e instructivos en materia de seguridad de la información.

7.5 El Sistema de Gestión de Seguridad de la Información (SGSI) se implementa para minimizar el riesgo en el desarrollo de las actividades más importantes del Ejército Nacional.

7.6 La información constituye uno de los recursos principales de una organización, por lo tanto, se le debe proteger, mediante un conjunto de actividades, controles y políticas de seguridad que se deben implementar con base a recursos humanos, hardware y software[41].

7.7 El Ejército Nacional brinda las pautas para fortalecer la cultura de seguridad de la información en los funcionarios, terceros y clientes.

7.8 Considerando la Guía 21 *"Gestión y Clasificación de Incidentes de Seguridad de la Información"*, versión 1.2[42]. del Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC, se determinarán como eventos de seguridad el "(…) *intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información o un impedimento en la operación normal de las redes, sistemas o recursos informáticos o una violación a una política de seguridad de la información (…)*".

8. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El modelo de Seguridad y privacidad de la Información (MSPI) está estructurado en cinco (5) fases que permiten a las entidades gestionar y mantener de forma adecuada la seguridad y privacidad de la información de sus activos de información. Estas fases se desarrollan de la siguiente manera:

1. **Diagnóstico**: se debe iniciar un diagnóstico o análisis de brechas (GAP), cuyo propósito es identificar su estado actual frente a los requisitos del MSPI.

---

[41] Vega Velasco, W. (2008). *Políticas y seguridad de la información*. Fides et Ratio, (ISSN 2071-081X).

[42] El objetivo principal del Modelo de Gestión de Incidentes de seguridad de la información es tener un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del Ministerio de Tecnologías de Información y Comunicaciones (MinTIC), https://gobiernodigital.mintic.gov.co/692/articles-150509_G21_Gestion_Incidentes.pdf

2. **Planificación**: se debe establecer las necesidades, objetivos y estrategias de seguridad y privacidad de la información, considerando el mapa de procesos, el tamaño institucional y el contexto interno y externo. Esta fase incluye la identificación, valoración y tratamiento de riesgos, siendo el pilar del ciclo de gestión.

3. **Operación**: en esta fase, la entidad implementa los controles definidos en la planificación para reducir la probabilidad y el impacto de los riesgos identificados.

4. **Evaluación del desempeño**: se mide la efectividad del modelo a través de auditorías, revisiones y análisis de indicadores definidos previamente, permitiendo identificar avances, desviaciones o áreas de mejora.

5. **Mejoramiento continuo**: se establecen mecanismos para detectar y corregir desviaciones, implementar acciones correctivas y prevenir su repetición, fortalecimiento así el sistema de manera progresiva.

Ilustración 4 *Diagnostico Análisis GAP*

Fuente: *Documento Maestro de los lineamientos del Modelo de seguridad de la información versión 5 de 2025 pag.6*

El Ejército Nacional de conformidad a la Resolución 500 del 10 de marzo de 2021[43], adopta el Modelo de Seguridad y Privacidad de la Información, como guía para implementar el Sistema de Gestión de Seguridad de la Información, alineado a la norma técnica ISO/IEC 27001:2022. A continuación, se presenta la estructura del Sistema de Gestión de Seguridad de la Información.

8.1 POLÍTICA GENERAL DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En la página web del Ejército Nacional www.ejército.mil.co se encuentra publicada la política general de la seguridad y privacidad de la información de acuerdo al formato (POL-JEMPP-CEDE6-008-V2), donde se indica que:

"El Ejército Nacional, con el fin de apoyar el cumplimiento de su misión Institucional, reconoce la importancia de establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información, con el fin de identificar y proteger sus activos de información, propendiendo por la disponibilidad, confidencialidad e integridad, enmarcado en la normatividad vigente y aplicable, y alineado con la misión, visión, objetivos estratégicos, principios y valores de la Institución, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos". (Cursiva fuera de texto)

8.2 ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI).

El Ejército Nacional establece e implementa el Sistema de Gestión de Seguridad de la Información (SGSI) para proteger la reserva legal, la confidencialidad, la integridad y la disponibilidad de los activos de información, mediante el cumplimiento de las políticas, procedimientos, controles y lineamientos de seguridad de la información definidos, los cuales deben ser conocidos, comprendidos y aceptados por todas las partes interesadas, garantizando los recursos necesarios para la mejora continua del sistema.

8.3 OBJETIVO GENERAL DEL SGSI

Establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI), con el propósito de garantizar la protección de la información y de los activos de información institucionales, asegurando su reserva legal, la confidencialidad, la integridad y la disponibilidad de la información

[43] "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"

y de los activos de información del Ejército Nacional, mediante la gestión sistemática de riesgos, el **cumplimiento del marco normativo aplicable** y la adopción de **controles de seguridad pertinentes, proporcionales y adecuados** a las necesidades operacionales y misionales de la Fuerza.

8.4 OBJETIVOS ESPECÍFICOS DEL SGSI

a. Garantizar el cumplimiento del marco normativo y legal vigente aplicable al Ejército Nacional en materia de seguridad de la información, protección de datos y privacidad, conforme a las disposiciones internas y externas que regulan la gestión de la información institucional.

b. Establecer e implementar políticas, procedimientos, controles y lineamientos institucionales orientados a la seguridad de la información, asegurando su adecuada aplicación en los procesos administrativos y operacionales del Ejército Nacional.

c. Gestionar de manera sistemática los riesgos asociados a la seguridad de la información, con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información, garantizando su protección frente a amenazas internas y externas.

d. Promover y consolidar una cultura institucional de seguridad de la información, mediante acciones permanentes de divulgación, capacitación y sensibilización dirigidas a las partes interesadas del SGSI, sobre políticas, lineamientos y normatividad vigente en materia de seguridad y privacidad.

e. Asegurar la gestión oportuna, efectiva y documentada de los incidentes de seguridad de la información, conforme a los procedimientos y controles establecidos, con el propósito de minimizar impactos sobre las actividades administrativas, operacionales y misionales del Ejército Nacional.

8.5 RESPONSABILIDAD DE SEGURIDAD DE LA INFORMACIÓN

Contribuir a la continuidad y disponibilidad de los servicios de Tecnologías de la Información (TI) del Ejército Nacional, fortaleciendo la resiliencia institucional y reduciendo vulnerabilidades que puedan afectar la operación y el cumplimiento de la misión constitucional.

La responsabilidad de seguridad de la información se articula de la siguiente

manera:

a. Resolución 00007722 del 25 de octubre de 2021[45] del Comité Institucional de Gestión y Desempeño Ejército Nacional.

b. Directiva Permanente 007870 del 26 de diciembre 2022[46] del Ministerio de Defensa.

8.6 INFORMACIÓN DOCUMENTADA

El Ejército Nacional tramita toda la información necesaria para dar cumplimiento al Sistema de Gestión de Seguridad de la Información, teniendo en cuenta la normatividad vigente aplicable y los requisitos a nivel documental que exige la norma ISO 27001:2022.

A continuación, se relacionan los procedimientos que hacen parte del Sistema de Gestión de Seguridad de la Información (SGSI) del Ejército Nacional, emitidos por el Departamento de Comunicaciones y el Departamento de Inteligencia y Contrainteligencia, así:

a. Procedimiento de Gestión de Activos de Información (P-JEMPP-CEDE6-331).
b. Procedimiento de Gestión de Acceso (P-JEMPP-CEDE6-332).
c. Procedimiento de Control de Acceso Áreas Seguras (P-JEMPP-CEDE6-323).
d. Procedimiento de Gestión de Incidentes de Seguridad de la Información (P-JEMPP-CEDE6-325).
e. Procedimiento de Recolección de Evidencia Digital (P-JEMPP-CEDE6-326).
f. Procedimiento de Criptografía (P-JEMPP-CEDE6-333).
g. Procedimiento de Transferencia de Información (P-JEMPP-CEDE6-324).
h. Procedimiento de Seguridad en Sistemas de Información C5 (P-JEMPP-CEDE6-327).
i. Procedimiento de Gestión de Medios Removibles (P-JEMPP-CEDE6-328).
j. Procedimiento de Derechos de Propiedad Intelectual (P-JEMPP-CEDE6-330).
k. Procedimiento de Registro Bases de Datos Personales Ante la Superintendencia de Industria y Comercio (P-JEMPP-CEDE6-445).
l. Procedimiento Anonimizarían de Datos Personales Estructurados (P-JEMPP-CEDE6-450).
m. Procedimiento Gestión de Copias de Respaldo (P-JEMPP-CEDE6-454).

[45] Por la cual se crea el Comité Institucional de Gestión y Desempeño, el Modelo Integrado de Planeación y Gestión, el Modelo Estándar de Control Interno, el Subcomité Central de Coordinación del Sistema de Control Interno en el Ejército Nacional de Colombia, se dictan otras disposiciones y se deroga la resolución N° 002420 de 2018 del 25 de octubre de 2018 "

46 "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".

n. Procedimiento de Mantenimiento del Plan de Recuperación Ante Desastres (DRP) (P-JEMPP-CEDE6-458).
o. Procedimiento de Evaluación del SGSI (P-JEMPP-CEDE6-329).
p. Procedimiento de Gestión de Cambios de Infraestructura Tecnológica (P-JEMPP-CEDE6-423).
q. Procedimiento de datos abiertos (P-JEMPP-CEDE6- P-JEMPP-CEDE6-508).
r. Procedimiento de datos personales (P-JEMPP-CEDE6-506).

Los procedimientos[48] anteriormente relacionados se encuentran publicados en la página de intranet del Ejército Nacional, y podrán ser consultados permanentemente por los Líderes de Proceso y demás funcionarios que requieran su aplicación.

9. ESTADO ACTUAL

El Ejército Nacional define el presente Plan de Trabajo en la vigencia 2026, utilizando como insumo las evaluaciones de seguridad, los resultados de gestión de riesgos e indicadores de cada vigencia.

De acuerdo con lo anterior, para verificar el cumplimiento de las exigencias del Sistema de Gestión de Seguridad de la Información (SGSI), se han realizado las siguientes acciones:

9.1 Verificación del cumplimiento de las Políticas de Gobierno Digital y Seguridad Digital por intermedio de la evaluación realizada por el Departamento Administrativo de la Función Pública (DAFP) mediante el Formulario Único de Reporte de Avances de la Gestión (FURAG), en el marco de Modelo Integrado de Planeación y Gestión (MIPG).

9.2 Seguimiento realizado por el Departamento de Planeación del Ejército (CEDE5), al cumplimiento de las políticas Gobierno Digital y Seguridad Digital a través de la suite visión empresarial.

9.3 Autoevaluación mediante la herramienta de diagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) suministrada por el Ministerio de Tecnologías de la Información y las Comunicaciones.

9.4 Fortalecimiento del Centro de Operaciones de Seguridad (SOC), mediante la renovación de herramientas de seguridad cibernética, destinadas a la

[48] Procedimientos del Sistema de Gestión de Tecnologías y Sistemas de Información C5.
http://intranet.ejercito.mil.co/s_i_g/procesos_procedimientos/procesos_sistema_gestion_calidad/gestion_tecnologias_sistemas_52363/52366&pag=1

protección contra ataques cibernéticos, contención de amenazas y gestión de eventos.

Conforme a lo anterior, se cuenta con el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) de la vigencia 2025, que es usado como base para la formulación de las actividades del presente plan de trabajo, orientadas a mejorar y fortalecer el Sistema de Gestión de Seguridad de la Información del Ejército Nacional, en alineación al Modelo de Seguridad y Privacidad de la Información, como se muestra a continuación:

Ilustración 5 *Diagnóstico Modelo de Seguridad y Privacidad de la Información (MSPI)*

	CONTROLES ISO 27001:2022	ACTUAL	OBJETIVO	MADUREZ
A5	CONTROLES ORGANIZACIONALES	80	100	OPTIMIZADO
A6	CONTROLES PERSONAS	90	100	OPTIMIZADO
A7	CONTROLES FISICOS	80	100	OPTIMIZADO
A8	CONTROLES TECNOLOGICOS	80	100	OPTIMIZADO
	TOTAL	**82,5**		

Fuente: *Dirección de Prospectiva e Innovación C5 (DIPIC)*

10. PLAN DE ACTIVIDADES DEL SISTEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para el seguimiento y evaluación del Sistema de Gestión de Seguridad de la Información en su implementación se realizarán las siguientes actividades:

Tabla 1 *Cronograma de actividades plan de acción*

ACTIVIDADES	ENTREGABLE	RESPONSABLE	PERIODICIDAD		
Elaborar el Plan Estratégico de seguridad y privacidad de la información	Plan Estratégico de seguridad y privacidad de la información	JEMPP-CEDE6	Anual	1/09/2026	15/12/2026
Modelo Integrado de Planeación y Gestión MIPG					
Elaborar el Autodiagnóstico de Seguridad y privacidad de la Información MSPI	Autodiagnóstico	JEMOP-CAOCC JEMIC -CACIM	Anual	2/09/2026	30/11/2026

Seguimiento "Lineamientos para el desarrollo de la Política General de Seguridad de la Información en el Ejército Nacional"	Informe o actas de reunión	JEMPP-CEDE6	Anual	1/04/2026	30/11/2026
Actualizar la Política de seguridad y privacidad de la Información	Política publicada intranet y página web www.ejercito.mil.co	JEMPP-CEDE6	Anual	1/04/2026	30/09/2026
Actualizar la Matriz de verificación requisitos legales de seguridad de la información	Normograma actualizado	JEMPP-CEDE6 (Jurídica)	Anual	1/08/2026	20/12/2026
Protección de datos abiertos					
Actualizar Lineamientos para la Política de Datos abiertos	Publicación Licencia abierta o condiciones de uso para datos abiertos	SECEJ-DANTE con apoyo de DICOE	Anual	1/04/2026	30/11/2026
Protección de datos personales					
Actualizar Lineamientos para la Política de datos personales	Aviso de seguridad y privacidad términos y condiciones de uso de sitio web, aplicación web (app) o medio digital para datos personales.	DICOE	Anual	1/04/2026	30/11/2026
Gestión de Riesgos de seguridad de la información					
Elaborar el Plan de tratamiento de riesgos de seguridad y privacidad de la información	Plan de tratamiento de riesgos de seguridad y privacidad de la información	JEMPP - CEDE6	Anual	1/09/2026	30/12/2026
Actualizar la Declaración de aplicabilidad.	Diligenciar la declaración de aplicabilidad de acuerdo a la ISO27001: 2022 para año 2026.	JEMOP – CAOCC JEMIC – CACIM	Anual	1/04/2026	30/11/2026
Gestión de activos de información					
Actualizar matriz de activos de información	Actualización matriz gestión de activos de información	JEMOP – CAOCC, JEMIC	Anual	1/04/2026	30/11/2026

Cambio y cultura de seguridad de la información					
Capacitación, sensibilización y comunicación de seguridad de la información	Informe capacitación de acuerdo a Plan capacitación Institucional de Capacitación (PIC)	JEMPP-CEDE6 CEDE2	Anual	1/04/2026	10/12/2026
Realizar auditoría interna de seguridad de la información	Plan o cronograma de auditorías internas del Ejército Nacional	COEJC-CEIGE	Anual	31/03/2026	10/12/2026
Plan de Continuidad del Negocio					
Plan de recuperación ante desastres (DRP) y Documentación análisis de impacto del negocio (BIA)	Documento Actualizado del plan de recuperación a desastres (DRP), BIA.	JEMOP-CAOOC JEMIC, CEDE2, CEDE6	Anual	1/03/2026	20/12/2026

Fuente: *Plan de Acción CEDE6*

11. INDICADORES DE SEGUIMIENTO

El seguimiento al presente Plan se realizará conforme al plazo indicado para cada una de las actividades establecidas y de conformidad a los lineamientos del Departamento de Planeación (CEDE5), para el uso de la plataforma Suite Visión Empresarial, conforme a la Directiva Permanente 00203 de 2017 *"Seguimiento y evaluación de la gestión y resultados para el Ejército Nacional bajo la metodología de Balance Scorecard"*.

Ante demoras en la ejecución o posibles incumplimientos, se deberá establecer las acciones de mejora que permitan alcanzar lo establecido en el Plan y/o ajustando lo necesario con su debida justificación. Por lo anterior, se establecen los siguientes indicadores para verificar el cumplimiento del Plan:

Tabla 2 *Indicadores de evaluación seguridad de la información.*

Nombre del indicador: GESTIÓN DE INCIDENTES CIBERNÉTICOS	
Meta: *Gestionar el 95% de los incidentes Cibernéticos*	
Tipo de indicador: *Eficiencia (EFCC)*	**Formula del indicador:** *(V1/V2) x100*
Variable 1 – V1: *Número de amenazas cibernéticas mitigadas y/o contenidas.* Fuente de información: *CAOCC y CAIMI*	**Variable 2 – V2:** *Número de amenazas cibernéticas detectadas.* Fuente de información: *CAOCC y CAIMI*
Evaluación: *trimestral*	**Tendencia:** *estable*

Fuente: *Departamento de Comunicaciones - Dirección de Prospectiva e Innovación C5 (DIPIC)*

12. NORMATIVIDAD DE REFERENCIA

a. Constitución Política de Colombia (1991)[49]
b. Ley 1273 del 05 de enero de 2009, "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
c. Ley 1581 del 17 de octubre de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales".
d. Decreto 2609 del 14 de diciembre de 2012, "Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
e. Decreto 1377 del 27 de junio de 2013, "Por el cual se reglamenta parcialmente la Ley 1581 de 2012". Derogado Parcialmente por el Decreto 1081 de 2015.
f. Decreto 886 del 13 de mayo de 2014, "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos ".
g. Decreto 103 del 20 de enero de 2015, "Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".
h. Decreto 767 del 16 de mayo de 2022 "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".
i. Decreto 338 del 8 de marzo de 2022 "Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones".
j. Resolución 007722 del 25 de octubre de 2021, "Por la cual se crea el Comité

[49] Constitución Política, (1991), art. 15 "derecho de protección de datos personales como el derecho de toda persona para conocer, actualizar, rectificar y/o cancelar la información y datos personales que de ella se hayan recolectado y/o se traten en bases de datos públicas o privadas".

Institucional de Gestión y Desempeño, el Modelo Integrado de Planeación y Gestión, el Modelo Estándar de Control Interno, el Subcomité Central de Coordinación del Sistema de Control Interno en el Ejército Nacional de Colombia, se dictan otras disposiciones y se deroga la resolución N°002420 de 2018 del 25 de octubre de 2018" emitida por el Ejército Nacional.

k. Reglamento Generador de Fuerza del Ejército Nacional RGE 4-0.1 (RGE), "Gestión Documental para el Ejército Nacional".

l. Directiva Permanente 7870 del 26 de diciembre de 2022, Ministerio de Defensa Nacional, "Por el 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".

m. Directiva Permanente 00196 del 27 de diciembre de 2017, Ejército Nacional, "Destrucción y disposición final de residuos de aparatos eléctricos electrónicos (RAEE)", la que la modifique, aclare o adicione.

n. Directiva Permanente 00200 del 27 de diciembre de 2017, Ejército Nacional, "Computación", la que la modifique, aclare o adicione.

o. Directiva Permanente 00203 del 27 de diciembre de 2017, Ejército Nacional, "Seguimiento y evaluación de la gestión y resultados para el Ejército Nacional bajo la metodología de Balanced Scorecard", la que la modifique, aclare o adicione.

p. Directiva Permanente 2025228010640103 del 16 de junio de 2025," Lineamientos para el desarrollo de la Política General de Seguridad de la información en el Ejercito Nacional".

q. Directiva Permanente 00115 del 03 de diciembre de 2019, Ejército Nacional, "Lineamientos generales para la administración de riesgos en el Ejército Nacional", la que la modifique, aclare o adicione.

r. Consejo Nacional de Política Económica y Social. Departamento Nacional de Planeación. Documento CONPES 3701 del 14 de julio de 2011 "Lineamientos de política para ciberdefensa y ciberseguridad.

s. Consejo Nacional de Política Económica y Social. Departamento Nacional de Planeación. Documento CONPES 3854 del 11 de abril de 2016, "Política Nacional de Seguridad Digital".

t. Consejo Nacional de Política Económica y Social. Departamento Nacional de

Planeación. Documento CONPES 3995 del 1 de julio de 2020, "Política Nacional de Confianza y Seguridad Digital".

u. Consejo Nacional de Política Económica y Social. Departamento Nacional de Planeación. Documento CONPES 4144 14 de febrero de 2025, "Política Nacional de Inteligencia Artificial".

v. Plan Estratégico Institucional 2022 - 2026 (PEI), "Hombres y Mujeres de Honor al Servicio de la Nación" del Departamento de Planeación CEDE5.

w. Guía metodológica para la administración de riesgos 2022 del Departamento de Planeación CEDE5.

Firma,

3962

Brigadier General RAFAEL HERNANDO JIMÉNEZ JIMÉNEZ
Jefe Departamento de Comunicaciones CEDE6

Elaboró: PD06. Deicy Díaz
Profesional Defensa CEDE6

Revisó.: CT. Orlando Rodríguez
Oficial Gestión de la Innovación C5 CEDE6

Revisó.: AS. Alejandra Betancourt
Asesora Jurídica CEDE6

Vo.Bo.: TC. Alessio Rodríguez
Director Prospectiva e Innovación C5 CEDE6