PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Departamento de Comunicaciones (CEDE6)

2024

NOMBRE DOCUMENTO	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
Código de formato Aprobado Departamento de Planeación (CEDE5)	PLIE-JEMPP-CEDE6-02	Versión 0	2019-01-31
Actualización contenido			30 / 01 / 2020
Actualización contenido			21 / 12 / 2021
Actualización contenido			15 / 01 / 2022
Actualización contenido			30 / 01 / 2023
Actualización contenido			30 / 01 / 2024

TABLA DE CONTENIDO

TABLAS

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 de Seguridad y Privacidad de la Información, que se integra al plan de acción institucional, de conformidad con el Decreto N° 612 del 04 de abril de 2018, *"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".*

Por consiguiente, este documento presenta el plan de trabajo a seguir en la vigencia 2024 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 N° 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*" y los establecidos en la Política Seguridad Digital, de acuerdo con la Resolución N° 00500 de marzo 10 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), "*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*".

Por lo anterior, el Ejército Nacional presenta a los grupos de interés y a la ciudadanía el Plan de Seguridad y Privacidad de la Información para la vigencia 2024, en el cual se establece un conjunto de actividades basadas en el Planear, Hacer, Verificar y Actuar (PHVA), para crear condiciones de uso confiable en el entorno digital y físico de la información, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información y el establecimiento de controles para mitigar las posibles afectaciones a los activos que apoyan la evaluación de los procesos institucionales, basado en el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones, así como en la Norma Técnica Colombiana NTC-ISO27001:2013 modificada por la Norma Técnica colombiana NTC-ISO27001:2022.

Con fundamento en estos parámetros, se podrá crear un ambiente de transparencia en gestión pública y seguridad digital. El desafío es lograr que la implementación del modelo planteado conduzca a una solución eficaz y eficiente, que permita mantener los niveles de seguridad de la información requeridos al interior de la Institución.

2. DEFINICIONES[1]

- **Activo:** 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[2].

- **Amenaza:** causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización[2].

- **Análisis de riesgo:** proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo[2].

- **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[2].

- **Bases de datos personales**: conjunto organizado de datos personales que sea objeto de Tratamiento [3].

- **Causa**: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo[4].

- **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados[2].

- **Control:** medida por la que se modifica el riesgo[2]. Las políticas, los procedimientos, las prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo[5].

---

[1] Las definiciones del presente plan se adoptan y alinean a las que presenta el Ministerio de Tecnologías de la Información y Comunicaciones, en su Modelo de Seguridad y Privacidad de la Información. MinTIC, versión 3.0.2. 29/07/2016.
[2] Tecnologías de la Información, técnicas de seguridad, Sistema de Gestión de Seguridad de la Información, descripción general y vocabulario, ISO/IEC 27000, 5ta edición, 2018.
[3] Ley 1581 del 17 de octubre de 2012, “Por el cual se dictan disposiciones generales para la protección de datos personales”, se estable como el “conjunto organizado de datos personales que sea objeto de Tratamiento”, artículo 3.
[4] Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, Departamento Administrativo de la Función Pública, versión 5, 2020.
[5] Modelo de Seguridad y Privacidad de la Información (MSPI), Ministerio de Tecnologías de la Información y Comunicaciones, versión 3.0.2, 2016.

- **Ciberseguridad:** se entiende como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales. La ciberseguridad tiene el fin de proteger a los usuarios y los activos de Estado en el Ciberespacio y comprende el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para dicho fin[6].

- **Ciberespacio:** es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios[7].

- **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[2].

- **Datos personales**: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables[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 sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva[3].

- **Datos personales privados**: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular[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

[6] CONPES 3995 del 1 de julio de 2020, Política Nacional de Confianza y Seguridad Digital.
[7] Comisión de Regulación de Comunicaciones, Resolución 2352 del 29 de enero de 2010, “Por la cual se modifican las Resoluciones CRT 1740 de 2007 y 1940 de 2008 y se dictan otras disposiciones”.

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[3].

- **Evaluación del riesgo de seguridad de la información:** medición y evaluación continua de amenazas, impacto y vulnerabilidades sobre los activos de información, que permita la minimización de la ocurrencia de dichos riesgos. Proceso global de identificación, análisis y estimación de riesgos[2].

- **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[2].

- **Impacto:** el coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros, por ejemplo la pérdida de reputación, implicaciones legales, etc[2].

- **Integridad**: propiedad de la información relativa a su exactitud y completitud[2].

- **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año[4].

- **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[2].

- **Privacidad:** el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades públicas, la correlativa obligación de proteger dicha información en observancia del marco legal vigente[5].

- **Riesgo**: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales[4].

- **Riesgo de seguridad de la información:** está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización[2].

- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información[2].

- **Sistema de Gestión de Seguridad de la Información (SGSI)**: conjunto de elementos interrelacionados (estructura organizativa, políticas, planificación de 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[2].

- **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[2].

- **Vulnerabilidad**: debilidad de un activo o control que puede ser explotada por una o más amenazas[2].

3. Objetivo

Establecer la estrategia para que los activos de la información del Ejército Nacional sean utilizados, clasificados y asegurados atendiendo a la normatividad vigente.

4. ALCANCE

El Ejército Nacional, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), mediante el cual la Fuerza establece un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos. Por lo tanto, para alcanzar dicha confianza, es necesario brindar la protección de la información institucional, mediante la implementación de controles que disminuyan la probabilidad e impacto de los riesgos que se identifiquen de manera sistemática, manteniendo un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la información.

Por lo tanto, el Sistema de Gestión de Seguridad de la Información (SGSI) establece controles que aplican para todos los procesos, funcionarios, terceros, proveedores y la ciudadanía en general, los cuales de acuerdo con sus expectativas y/o necesidades, en cumplimento de sus funciones o de su interacción, comparten, utilizan, recolectan, procesan, intercambian o consultan información de la Institución.

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 de "*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*"[8]. Igualmente, este sistema considera la visión, objetivos estratégicos y lineamientos del Sistema Integrado de Gestión del Ejército Nacional.

Por consiguiente, el SGSI dispone los lineamientos de seguridad y privacidad de la información, orientados a preservar la integridad, disponibilidad y confidencialidad de la información, de acuerdo con la estructura documental y los lineamientos del Sistema Integrado de Gestión, que a su vez está alineado al Sistema de Gestión de Calidad, permitiendo responder a todas las necesidades y requisitos de obligatorio cumplimiento, así como fortalecer los procesos y optimizar los recursos en la Institución.

[8] Misión Institucional del Ejército Nacional de Colombia.

Adicionalmente, el Ejército Nacional de Colombia se encuentra integrado por tres Jefaturas de Estado Mayor, que cumplen los direccionamientos del Gobierno Nacional, y seguirán los lineamientos establecidos para el SGSI, de acuerdo con la siguiente organización jerárquica:

Ilustración 2. *Organigrama del Ejército Nacional de Colombia*

Fuente: *Ejército Nacional de Colombia, disponible en página web Ejército Nacional https://www.ejercito.mil.co/organigrama/*

Con la finalidad de ampliar la implementación de los lineamientos del SGSI, se tendrá el apoyo de los Oficiales de Comunicaciones y de Seguridad Militar de las Unidades del escalón Táctico a nivel División, para que orienten el cumplimiento de los controles de seguridad en sus Unidades subalternas.

6. PREMISAS

El presente plan responde a las necesidades institucionales de seguridad de la información, por lo cual propende por fortalecer la implementación del SGSI, teniendo en cuenta las siguientes premisas:

A. El Plan cumple 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.

B. 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".

C. El Ejército Nacional propende por el apoyo en la innovación tecnológica, la cual es fundamental en la toma de decisiones con respecto al SGSI.

D. El SGSI emite las políticas, procedimientos e instructivos en materia de seguridad de la información.

E. El SGSI se implementa para minimizar el riesgo en el desarrollo de las actividades más importantes del Ejército Nacional.

F. 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[9].

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

H. Considerando la Guía N° 21 del 6 de noviembre de 2016 *"Gestión y Clasificación de Incidentes de Seguridad de la Información",* versión 1.2. del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), se determinarán como eventos de seguridad el "intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información o

[9] Políticas y Seguridad de la Información, Walter Vega Velasco, Fides Et Ratio 2008, ISSN 2071-081X.

un impedimento en la operación normal de las redes, sistemas o recursos informáticos o una violación a una política de seguridad de la información".

7. PRINCIPIOS

Los principios de seguridad que soportarán el SGSI del Ejército Nacional, se elaboran a partir de la norma ISO 27001:2013 modificada por la norma ISO 27001:2022, y la Guía N° 2 "*Elaboración de la Política General de Seguridad y Privacidad de la Información*" del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC).

Por ello, de acuerdo con las necesidades y características del Ejército Nacional, se definen los siguientes principios:

A. DISPONIBILIDAD: los activos de información estarán disponibles cuando se requieran por parte de los usuarios autorizados.

B. INTEGRIDAD: se evitará la modificación no autorizada a la información, asegurando su exactitud, completitud y veracidad.

C. CONFIDENCIALIDAD: se permitirá el acceso a los activos de información únicamente a los usuarios autorizados. El acceso a los activos según su nivel de clasificación será concedido a través de mecanismos con diferentes niveles de complejidad, que permita garantizar que quien lo está accediendo es quien dice ser y se encuentra autorizado.

D. RESERVA LEGAL: se mantendrá la restricción que por mandato legal exista para conocer o acceder a la información que posee un documento, ya sea público o privado.

E. AUTENTICACIÓN: a partir de una autenticación exitosa se determinará a qué recursos puede acceder o usar un usuario a partir de su identidad, los cuales deben ser los mínimos necesarios para el desarrollo de sus funciones.

F. GESTIÓN DE RIESGOS: es indispensable una constante identificación, valoración y tratamiento de riesgos de seguridad de la información asociados a los activos de información y su correspondiente seguimiento para validar el cumplimiento de los planes de tratamiento.

G. LEGALIDAD: el Ejército Nacional cumplirá con las obligaciones legales, regulatorias y contractuales establecidas en temas de seguridad y privacidad de la información.

H. RESPONSABILIDAD: todos los funcionarios y demás terceros son responsables de cumplir con las responsabilidades frente a la seguridad de la información.

I. **GESTIÓN DE INCIDENTES:** se realizará una identificación y reporte oportuno de los eventos e incidentes de seguridad, y las debilidades asociadas de los activos de información, con el fin de dar una respuesta efectiva y oportuna, para mitigar el impacto y poder a partir de las lecciones aprendidas mejorar el SGSI.

J. **MEJORA CONTINUA:** se revisarán periódicamente los controles de seguridad para validar que el SGSI esté implementado y mantenido eficazmente, validando el cumplimiento, desviaciones o incumplimientos del SGSI, y así definir acciones de mejora.

K. **NO REPUDIO O IRRENUNCIABILIDAD:** capacidad de demostrar o probar la participación de las partes (origen y destino, emisor y receptor, remitente y destinatario), mediante su identificación, en una comunicación o en la realización de una determinada acción.[10]

8. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Ejército Nacional de conformidad a la Resolución N°500 del 10 de marzo de 2021 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), "*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*", 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 27001:2013 modificada por la norma ISO/IEC 27001:2022. A continuación, se presenta la estructura del Sistema de Gestión de Seguridad de la Información.

A. Política general de la seguridad y privacidad de la información

"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" (POL-JEMPP-CEDE6-008-V1).

[10] https://www.google.com/search?q=capacidad+de+demostrar+o+probar+la+participaci%C3%B3n+de+las+partes

B. Finalidad de implementar el 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), en cumplimiento por la reserva legal, confidencialidad, integridad y disponibilidad de los activos de información, el cual exige el cumplimiento de la política general y políticas específicas de seguridad de la información, procedimientos, controles y demás lineamientos de seguridad de la información que se definan, los cuales deben ser conocidos, entendidos y aceptados por todas las partes interesadas del SGSI, garantizando los recursos necesarios para la mejora continua del sistema.

C. Objetivo general del SGSI

Preservar la reserva legal, confidencialidad, integridad y disponibilidad de los activos de información del Ejército Nacional.

D. Objetivos específicos del SGSI

1. Cumplir con el marco normativo y legal vigente, aplicable al Ejército Nacional en temas de seguridad y privacidad de la información.

2. Implementar políticas, procedimientos, controles y lineamientos de seguridad de la información.

3. Gestionar los riesgos de seguridad de la información, con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información.

4. Crear y mantener una cultura de seguridad de la información, a través de la divulgación y sensibilización de las políticas, lineamientos y demás normatividad vigente en temas de seguridad y privacidad a todas las partes interesadas al SGSI.

5. Resolver de manera precisa, oportuna y efectiva, los incidentes de seguridad de la información siguiendo los procedimientos, controles y lineamientos definidos, con el fin de reducir el impacto en las actividades administrativas y operativas del Ejército Nacional.

6. Contribuir a la continuidad y operación de los servicios de TI del Ejército Nacional.

E. Responsabilidad de seguridad de la información

La responsabilidad de seguridad de la información es liderada por el Comité Institucional de Gestión y Desempeño del Ejército Nacional, conformado a través de la Resolución N° 00007722 del 25 de octubre de 2021, emitida por el Comandando del Ejército Nacional o norma que la modifique o derogue.

Adicionalmente, el Ministerio de Defensa Nacional por intermedio de la Directiva Permanente N° 7870 del 26 de diciembre 2022, "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".

F. Información documentada

El Ejército Nacional documenta 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 27001:2013 modificada por la norma ISO 27001:2022.

A continuación, se relacionan los procedimientos que hacen parte del SGSI, así:

1. Gestión de Activos de Información
2. Gestión de Acceso
3. Control de Acceso Áreas Seguras
4. Gestión de Incidentes de Seguridad de la Información
5. Recolección de Evidencia Digital.
6. Criptografía.
7. Transferencia de Información.
8. Seguridad en Sistemas de Información C5
9. Gestión de Medios Removibles.
10. Derechos de Propiedad Intelectual.
11. Registro Bases de Datos Personales Ante la Superintendencia de Industria y Comercio.
12. Anonimización de Datos Personales Estructurados
13. Gestión de Copias de Respaldo.
14. Mantenimiento del Plan de Recuperación Ante Desastres (DRP).
15. Evaluación del SGSI.
16. Gestión de Cambios de Infraestructura Tecnológica.
    Computación.

Los procedimientos se encuentran disponibles para su consulta en el portal web institucional y en la intranet https://intranet.ejercito.mil.co/

9. ESTADO ACTUAL

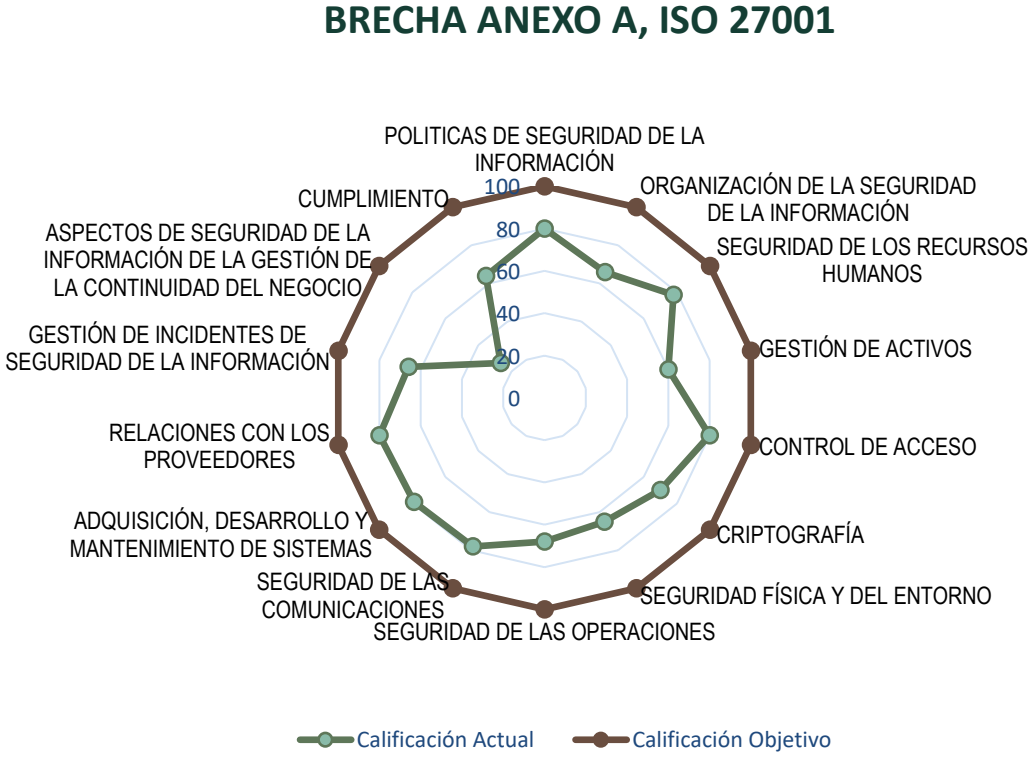
El Ejército Nacional define el presente Plan de Trabajo de acuerdo al análisis de la situación actual, utilizando como insumo las evaluaciones de seguridad, los resultados de gestión de riesgos e indicadores de cada vigencia.

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:

- Auditorías internas por medio de inspecciones lideradas por la Inspección General del Ejército Nacional.
- Verificación del cumplimiento de las Políticas de Gobierno Digital y Seguridad 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).
- Seguimiento realizado por el Departamento de Planeación del Ejército (CEDE5), al cumplimiento de las políticas Gobierno Digital y Seguridad Digital.
- Autoevaluación detallada 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.
- Actualización de la política general y lineamientos del sistema de gestión de seguridad y privacidad de la información.
- Fortalecimiento del Centro de Operaciones de Seguridad (SOC), mediante la renovación de herramientas de seguridad cibernética, destinadas a la 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 2023, 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 2**. Diagnóstico Modelo de Seguridad y Privacidad de la Información (MSPI)*



Fuente: Dirección de Planeación y Políticas C5 (DIPOC).

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 seguridad y privacidad de la información.*

Actividades	Entregable	Responsable	Periodicidad		
Elaborar el Plan de seguridad y privacidad de la información para año 2025.	Plan de seguridad y privacidad de la información para año 2025.	JEMPP-CEDE6	Anual	2/09/2024	30/12/2024
Modelo Integrado de Planeación y Gestión MIPG					
Elaborar el Autodiagnóstico de Seguridad y privacidad de la Información MSPI	Autodiagnóstico	JEMOP CAOOC con apoyo de CACIM	Anual	2/09/2024	22/11/2024
Emitir la Resolución del Comité Institucional de Gestión y Desempeño 2023 o	Resolución del Comité Institucional de Gestión y Desempeño con	JEMPP-CEDE5	Anual	01/03/2024	30/09/2024

Actualizar la Resolución 00007722 del 25 de octubre de 2021 del Comité Institucional de Gestión y Desempeño.	modificaciones de año 2023 o 2024.				
Modelo Integrado de Planeación y Gestión MIPG					
Actualizar o modificar la Política de seguridad y privacidad de la Información para el año 2024.	Política Actualizada 2024.	JEMPP-CEDE6	Anual	01/04/2024	30/09/2024
Actualizar Matriz de verificación requisitos legales de seguridad de la información	Normograma actualizado.	JEMPP-CEDE6 (Jurídica)	Anual	1/08/2024	20/12/2024
Protección de datos abiertos					
Elaborar Políticas y lineamientos para Datos abiertos año 2024.	- Políticas y lineamientos actualizados de datos abiertos 2024. - Licencia abierta o condiciones de uso para datos abiertos 2024.	SECEJ-DANTE-con apoyo de DICOE	Anual	1/04/2024	28/06/2024
Protección de datos personales					
Elaborar políticas y lineamientos para datos personales año 2024.	1. Política Actualizada de datos personales para año 2024. 2. Procedimiento actualizado para datos personales año 2024. 3. Aviso de seguridad y privacidad términos y condiciones de uso del sitio web, aplicación web (app) o medio digital para datos personales	JEMPP-CEDE1	Anual	1/04/2024	30/09/2024
Gestión de Riesgos de seguridad de la información					
Elaborar el Plan de tratamiento de riesgos de seguridad y privacidad de la información para año 2025.	Plan de tratamiento de riesgos de seguridad y privacidad de la información	JEMPP-CEDE6	Anual	2/09/2024	30/12/2024
Diligenciar la declaración de aplicabilidad de acuerdo a la ISO27001: 2022 para año 2024.	Declaración de aplicabilidad con soportes y respectivo Informe de seguimiento de aplicabilidad de la Seguridad de la Información	JEMPP JEMOP-CEDE2 CAOCC	Anual	1/04/2024	29/11/2024
Gestión de activos de información					
Actualizar matriz de activos de información	Documento con matriz de activos de información actualizada	JEMPP-CEDE2	Anual	8/04/2024	38/08/2024
Cambio y cultura de seguridad de la información					
Elaborar el plan de capacitación, sensibilización y comunicación de seguridad de la información para el año 2024.	Plan institucional de capacitación en la cual se evidencie la difusión de la seguridad de la Información	JEMPP-CEDE7	Anual	1/01/2024	30/12/2024

Elaborar el plan de implementación sede electrónica del Ejército Nacional de acuerdo art. 15 del Decreto 2106 de 2019	Plan de implementación sede electrónica del Ejército Nacional 2024 – 2025.	COEJC-DICOE, CAOCC	Anual	1/01/2024	29/11/2024
Plan de Continuidad del Negocio					
Elaborar análisis de impacto de la operación para año 2024.	Actualización Análisis de impacto del Negocio (BIA)	JEMPP - JEMOP CAOOC con apoyo de CACIM	Anual	08/04/2024	30/05/2024
Documentación plan de recuperación a desastres	documento con plan de recuperación a desastres actualizado	JEMOP CAOOC con apoyo de CACIM	Anual	1/04/2024	29/10/2024

Fuente: *Dirección de Planeación y Políticas C5*

11. Indicadores de seguimiento

El seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) se realizará conforme al plazo indicado para cada una de las actividades establecidas en el cronograma de que trata el numeral 10 del presente plan y los lineamientos del Departamento de Planeación (CEDE5), para el uso de la plataforma Suite Visión Empresarial, según la Directiva Permanente N° 00203 de 2017 “Seguimiento y evaluación de la gestión y resultados para el Ejército Nacional bajo la metodología de Balance Scorecard”.

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)	**Fórmula 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 Planeación y Políticas C5*

12. Normatividad de referencia

1) Constitución Política de Colombia (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”.

2) Ley 1273 del 05 de enero de 2009, Congreso de Colombia, “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”.

3) Ley 1581 del 17 de octubre de 2012, Congreso de Colombia, “Por la cual se dictan disposiciones generales para la protección de datos personales”.

4) Decreto N° 2609 del 14 de diciembre de 2012, Presidencia de la República de Colombia, “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”.

5) Decreto N° 1377 del 27 de junio de 2013, Presidencia de la República, “Por el cual se reglamenta parcialmente la Ley 1581 de 2012”, art. 20., derogado parcialmente por el Decreto 1081 de 2015, derogado parcialmente por el Decreto 1081 de 2015.

6) Decreto N° 886 del 13 de mayo de 2014, Presidencia de la República de Colombia, “Por el cual se reglamenta el Registro Nacional de Bases de Datos”.

7) Decreto N° 103 del 20 de enero de 2015, Presidencia de la República de Colombia, “Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”.

8) Decreto N° 767 del 16 de mayo de 2022, Presidencia de la República de Colombia, “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”.

9) Decreto N° 1389 del 28 de julio de 2022, Función Pública, “Por el cual se adicional el Título 24 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 la gobernanza en la infraestructura de datos y se crea el Modelo de gobernanza de la infraestructura de datos”.

10) Resolución N° 000460 del 15 de febrero de 2022, Ministerio de Tecnologías de la Información y las Comunicaciones, “Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación”.

11) Resolución N° 007722 del 25 de octubre de 2021, Ejército Nacional, Departamento de Planeación. “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”.

12) Resolución N° 7870 de 2022 del 26 de diciembre de 2022, Ejército Nacional, Departamento de Planeación. “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 la Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa”.

13) Reglamento Generador de Fuerza del Ejército Nacional RGE 4-0.1 (RGE), “Gestión Documental para el Ejército Nacional”.

14) Manual Operativo Sistema de Gestión, Modelo Integrado de Planeación y Gestión (MIPG), versión 2 de 2018 de la Función Pública.

15) Directiva Permanente N° 00196 del 27 de diciembre de 2017, Ejército Nacional, Departamento de Comunicaciones. “Destrucción y disposición final de residuos de aparatos eléctricos electrónicos (RAEE)”, la que modifique, aclare o derogue.

16) Directiva Permanente N° 00200 del 27 de diciembre de 2017, Ejército Nacional, Departamento de Comunicaciones. “Computación”, la que modifique, aclare o derogue.

17) Directiva Permanente N° 00201 del 27 de diciembre de 2017, Ejército Nacional, Departamento de Comunicaciones. “Lineamientos de Ciberseguridad y Ciberdefensa para el Ejército Nacional”, la que modifique, aclare o derogue.

18) Directiva Permanente N° 00203 del 27 de diciembre de 2017, Ejército Nacional, Departamento de Comunicaciones. “Seguimiento y evaluación de la gestión y resultados para el Ejército Nacional bajo la metodología de Balanced Scorecard”, la que modifique, aclare o derogue.

19) Directiva Permanente N°00221 del 27 de diciembre de 2017, Ejército Nacional, Departamento de Inteligencia y Contrainteligencia. “Lineamientos para el apoyo de la seguridad de la información del Ejército Nacional”, la que modifique, aclare o derogue.

20) Directiva Permanente N° 03 del 23 de enero de 2019, Ministerio de Defensa Nacional, Departamento de Inteligencia y Contrainteligencia. “Lineamientos para la definición de la Política de Tratamiento de Datos Personales en el Ministerio de Defensa”, la que la modifique, aclare o derogue.

21) Directiva Permanente N° 000027 del 06 de marzo de 2019, Ejército Nacional, “Lineamientos para la protección de la Propiedad Intelectual en el Ejército Nacional”.

22) Directiva Permanente N° 00115 del 03 de diciembre de 2019, Ejército Nacional, Departamento de Planeación. “Lineamientos generales para la administración de riesgos en el Ejército Nacional”, la que modifique, aclare o derogue.

23) Documento CONPES 3701 del 14 de julio de 2011, Consejo Nacional de Políticas Económica y Social de la República de Colombia, “Lineamientos de Política para Ciberseguridad y Ciberdefensa”.

24) Documento CONPES 3854 del 11 de abril de 2016, Consejo Nacional de Políticas Económica y Social de la República de Colombia, “Política Nacional de Seguridad Digital”.

25) Documento CONPES 3995 del 1 de julio de 2020, Consejo Nacional de Políticas Económica y Social de la República de Colombia, “Política Nacional de Confianza y Seguridad Digital”.

DEBIDAMENTE FIRMADO

13. BIBLIOGRAFÍA

Departamento Administrativo de la Función Pública. (2018). *Principios de la Administración Administrativa*. Obtenido de https://www.funcionpublica.gov.co/eva/gerentes/Modulo4/tema-1/3-principios.html

Departamento Administrativo de la Función Pública. (2022). *Guía para la administración del riesgo y el diseño de controles en Entidades Públicas.* Bogotá: DAFP.

International Organization for Standardization. (2018). *ISO-IEC 27000 Tecnologías de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión general y vocabulario.* Suiza: ISO. Obtenido de https://www.iso.org/standard/73906.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (11 de Mayo de 2016). *Modelo de seguridad MINTIC Guía 2 Política General MSPI V1.* Obtenido de https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

Ministerio de Tecnologías de la Información y las Comunicaciones. (29 de Julio de 2016). *Modelo de Seguridad y Privacidad de la Información.* Obtenido de https://mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf