PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EJÉRCITO NACIONAL DE COLOMBIA

Departamento de Comunicaciones (CEDE6)

2026

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

1. INTRODUCCIÓN

Las medidas preventivas y reactivas aplicadas sobre los sistemas tecnológicos institucionales constituyen un componente esencial para garantizar la protección de la información del Ejército Nacional frente a amenazas, vulnerabilidades y posibles brechas de seguridad que comprometan los principios de confidencialidad, integridad y disponibilidad. En este sentido, la adopción de controles de seguridad permite gestionar de manera estructurada los riesgos identificados, reducir su probabilidad de ocurrencia y mitigar los impactos que puedan afectar los activos de información y la continuidad de los procesos misionales y administrativos.

Por consiguiente, el presente Plan se elabora con el fin de dar a conocer cómo se realizará la gestión y socialización de los riesgos asociados a la seguridad de la información y así dar cumplimiento a la normativa establecida por el Estado colombiano, en especial del documento CONPES 3995 de 2020, "Confianza y Seguridad Digital", el Decreto 767 del 16 de mayo de 2022[1], y el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Adicionalmente, para fortalecer el enfoque técnico y garantizar la alineación con estándares reconocidos, el Plan incorpora buenas prácticas y lineamientos derivados de la NTC-ISO/IEC 27001:2022, así como de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (versión 6) expedida por el Departamento Administrativo de la Función Pública (DAFP) en noviembre de 2022, asegurando un tratamiento integral, proporcional y documentado de los riesgos en el marco del Sistema de Gestión de Seguridad de la Información (SGSI).

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

Archivo: conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o

[1] "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital para Colombia 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"

[2] 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. 8.

privada, en el transcurso de su gestión, y que se encuentran conservados respetando un orden definido, para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia.

También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura[3].

Amenaza: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización[4]. (ISO/IEC 27001:2022).

Análisis de riesgo: proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo[5]. (ISO/IEC 27001:2022).

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo[6].

Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.[7]

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.[8]

Contexto interno y externo: es necesario desplegar un análisis interno y externo específico para la entidad, donde se expliquen mediante información institucional formalizada y datos específicos relacionados.[9]

Control: 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

[3] Colombia. Congreso de la República. Ley 594 de 2000 (14 de julio), "Por medio de la cual se dicta la Ley General de Archivos". Artículo 3. Diario Oficial No. 44.084.
[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, pág. 8.
[5] Ibidem. Pág. 8
[6] Departamento Administrativo de la Función Pública (DAFP), Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5, 2020, pág. 14.
[7] Departamento Administrativo de la Función Pública (DAFP), Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 6, 2022, pág. 15.
[8] Departamento Administrativo de la Función Pública (DAFP), Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 6, 2022, pág. 14.
[9] Departamento Administrativo de la Función Pública (DAFP). Guía para la Gestión Integral del riesgo en Entidades Públicas versión 7, 2025, pág. 26.[10] Modelo de Seguridad y Privacidad de la Información (MSPI), Ministerio de Tecnologías de la Información y Comunicaciones, versión 4, 2021, pág. 12.

salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo[10].

Disponibilidad: es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona, entidad o proceso autorizada cuando así lo requiera esta, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso. de estar accesible.[11]

Declaración de aplicabilidad: es un documento formado por la relación completa de los controles de seguridad de la información evaluables, que se indican en el anexo A de la norma.[12]

Evaluación del riesgo: probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE)[13].

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[14].

Impacto estratégico: nivel de exposición a riesgos de seguridad y privacidad de la información[15].

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 destrucción no autorizada, asegurando que la información sea precisa y consistente durante todo su ciclo de vida[16].

Probabilidad: posibilidad de ocurrencia del riesgo, este puede ser medida con criterios de frecuencia o factibilidad.[17]

---

[10] Modelo de Seguridad y Privacidad de la Información (MSPI), Ministerio de Tecnologías de la Información y Comunicaciones, versión 4, 2021, pág. 12.
[11] Ministerio de Tecnologías de la Información y las Comunicaciones, Modelo de Seguridad y Privacidad de la Información, Versión 4, 2021, Seguridad y Privacidad de la Información, pág. 62.
[12] https://www.globalsuitesolutions.com/es/soa-declaracion-aplicabilidad/
[13] Departamento Administrativo de la Función Pública (DAFP), Guía para la Administración del Riesgo y el diseño de controles en entidades públicas versión 6. Pág. 44.
[14] International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements (Annex A: Controls 5.24, 5.26, 5.27, 6.8).
[15] Ministerio de tecnologías de la información y las comunicaciones, Documento Maestro de los lineamientos del Modelo de Seguridad y Privacidad de la Información Versión 5. Pág. 26.
[16] Integridad de la información en seguridad informática (2023, 22 agosto), https://www.hostdime.la/blog/integridad-de-la-informacion-en-seguridad-informatica/
[17] Guía para la Administración del Riesgo y el diseño de controles en entidades públicas versión 6. Pág. 75.

Plan de tratamiento de riesgos: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma[18].

Privacidad: facultad de una persona de prevenir la difusión de datos pertenecientes a su vida privada, sin ser difamatorios ni perjudiciales, esta desea que no sean divulgados[19].

Riesgo: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.[20]

Riesgo Corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado[21].

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.[22]

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información[23]. (ISO/IEC 27001:2022).

Sistema de Gestión de Seguridad de la Información (SGSI): conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001.[24]

Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas. [25](ISO/IEC 27000).

---

[18] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Modelo de Seguridad y Privacidad de la Información (MSPI), versión 4, 2021, pág. 14.
[19] Diccionario Panhispánico del español Jurídico, https://dpej.rae.es/lema/privacidad
[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. 17.
[21] Departamento Administrativo de la Función Pública (DAFP), Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 6, 2022, pág. 12.
[22] 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.
[23] 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.
[24] WIKIPEDIA, ENCICLOPEDIA LIBRE, https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n
25 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 GENERAL

Gestionar de manera integral y sistemática los riesgos asociados a la seguridad y privacidad de la información en los procesos institucionales del Ejército Nacional, mediante la implementación de medidas de tratamiento y controles adecuados, que permitan a los líderes de proceso asegurar la confidencialidad, integridad y disponibilidad de la información institucional, garantizando su protección frente a amenazas, vulnerabilidades y posibles incidentes de seguridad.

4. OBJETIVOS ESPECÍFICOS

4.1. Realizar el seguimiento, evaluación y medición periódica de los riesgos de seguridad y privacidad de la información asociados a los procesos tecnológicos del Ejército Nacional, mediante el uso y actualización de la herramienta tecnológica Suite Visión Empresarial, con el fin de asegurar su adecuada gestión y trazabilidad institucional.

4.2. Fortalecer la implementación y efectividad de los controles de seguridad de la información establecidos en el marco del Sistema de Gestión de Seguridad de la Información (SGSI), con el propósito de mitigar los riesgos identificados y reducir la probabilidad e impacto de incidentes que afecten la confidencialidad, integridad y disponibilidad de la información institucional.

5. ALCANCE

La gestión de riesgos de seguridad y privacidad de la información será aplicable a todos los servidores públicos del Ejército Nacional, tanto militares como civiles, así como a contratistas, proveedores, operadores y demás terceros que, en desarrollo de funciones, actividades o procesos institucionales, tengan acceso, administren, compartan, utilicen, recolecten, almacenen, procesen, transmitan, intercambien o consulten información de la Institución.

Asimismo, el presente alcance comprende a los entes de control y a las entidades relacionadas que, en ejercicio de sus competencias, accedan de manera interna o externa a cualquier activo de información del Ejército Nacional, incluyendo archivos físicos o digitales, bases de datos, plataformas tecnológicas, aplicaciones, software, repositorios institucionales, servicios en la nube u otros medios de almacenamiento y procesamiento, independientemente de su ubicación o forma de acceso.

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.[26]

Considerando que para la formulación del Plan Estratégico Institucional se tuvo en cuenta la Constitución Política de la República de Colombia (CPC[27]), el Plan Nacional de Desarrollo 2022 – 2026" (PND[28]), 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,[29] el Plan Estratégico Institucional del Comando General de las Fuerzas Militares, el Plan Estratégico Militar de Transformación (PEMT2042[30]) y los Diálogos Regionales Vinculantes (DRV[31]) 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 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.

---

[26] Plan Estratégico Institucional PEI 2022-2026, https://www.ejercito.mil.co/plan-estrategico-institucional-pei-2022-2026/

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

[28] Plan Nacional de Desarrollo 2022-2026 (2023, mayo), https://colaboracion.dnp.gov.co/CDT/Prensa/Publicaciones/plan-nacional-de-desarrollo-2022-2026-colombia-potencia-mundial-de-la-vida.pdf

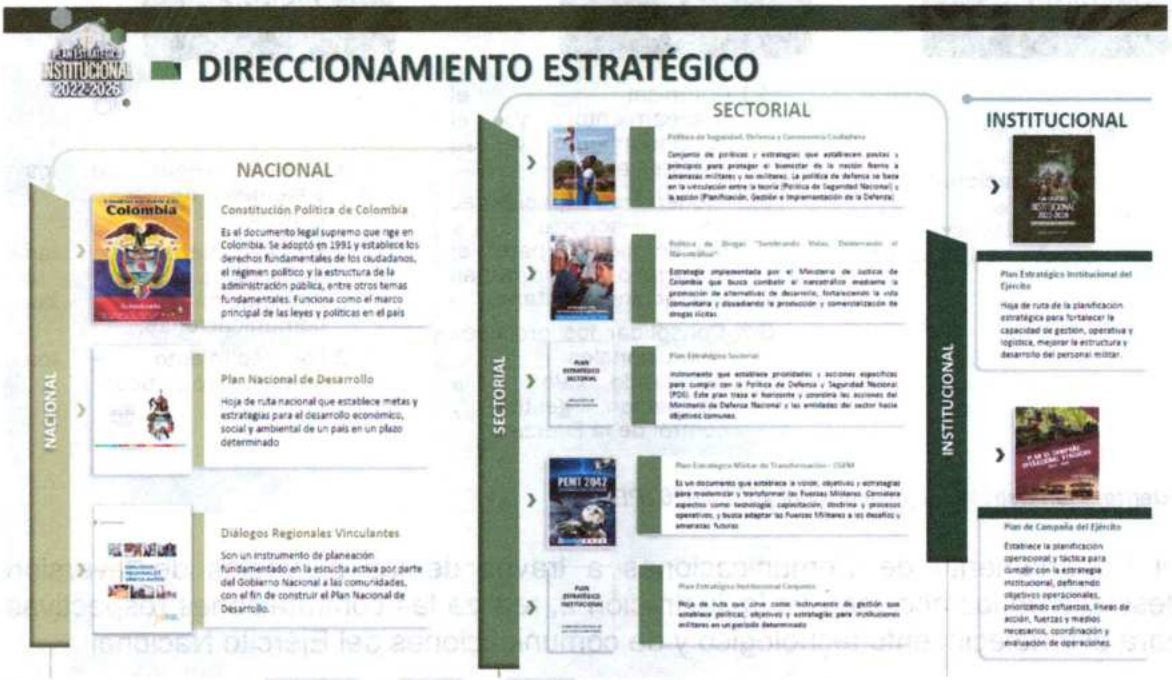
[29] Plan Estratégico del Sector Defensa y Seguridad, Guía de Planeamiento Estratégico (2022-2026), https://www.casur.gov.co/wp-content/uploads/2025/10/PES2024_MDN.pdf

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

[31] DNP, Colombia Tienes la Palabra, https://dialogosregionales.dnp.gov.co/

La siguiente gráfica presenta el marco de referencia normativo y estratégico que orienta la planeación institucional, evidenciando la articulación y jerarquía entre los distintos instrumentos de planificación del Estado.

Ilustración 1 *Alineación Estratégica Ejército Nacional.*



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

Frente al Plan Estratégico Institucional (PEI) 2022-2026, los objetivos estratégicos de TI orientados a fortalecer la infraestructura TIC institucional, apoyan directamente al cumplimiento de los objetivos estratgicos del Ejército Nacional consignados en el Plan Estratégico Institucional, en el numeral *6 "Fortalecer la estructura organizacional, procesos, capacidades y prácticas de gestión"*, el cual se materializa a través de los cursos de acción que se relacionan:

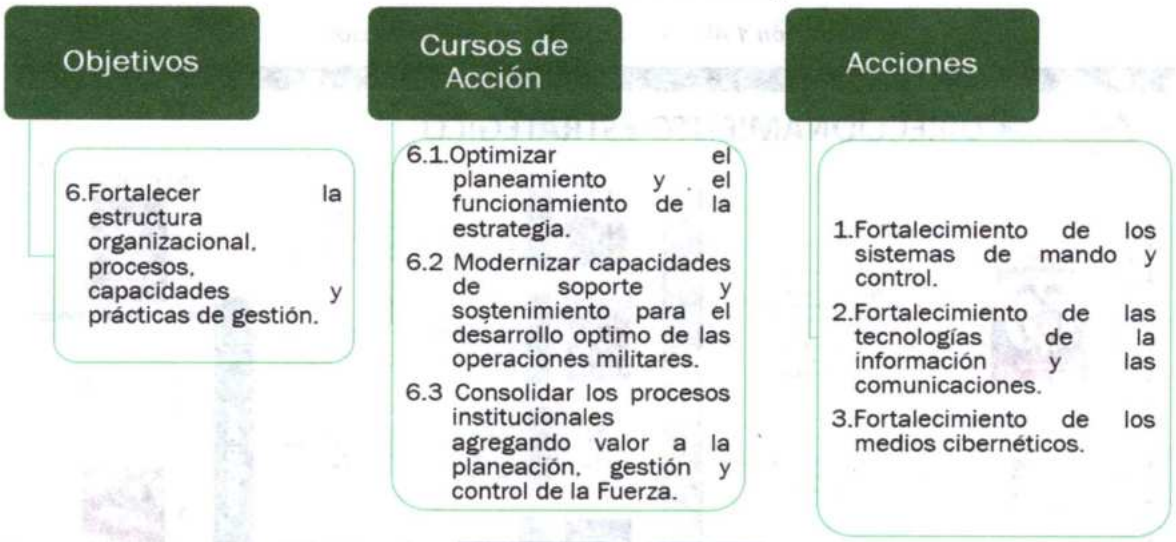
1. Optimizar el planeamiento y el funcionamiento de la estrategia.

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.

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 2** Aportes TIC a la Estrategia.*



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

El Departamento de Comunicaciones a través de los proyectos de inversión descritos en las acciones de la ilustración 2, realiza las contrataciones respectivas para el fortalecimiento tecnológico y de comunicaciones del Ejército Nacional.

7. RECURSOS

El Ejército Nacional, en el marco de la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción), dispone de los siguientes recursos:

7.1 Humano: Representantes institucionales, líderes del proceso (administración de infraestructura tecnológica, bases de datos, sistemas de información, gestión telemática, almacenamiento, disponibilidad, transmisión, entre otros), profesionales en tecnología, personal interno y personal externo.

7.2 Físico: Infraestructura tecnológica y equipos de comunicación.

7.3 Financiero: Planes de compras anuales institucionales.

7.4 Técnico: La metodología establecida en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 7,

Departamento Administrativo de la Función Pública (DAFP), noviembre 2025.

8. RESPONSABLES DE LA GESTIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

8.1 Líderes de Proceso que deben propender por la protección de los datos, implementar las políticas, gestionar los riesgos y fomentar una cultura de ciberseguridad, supervisar el cumplimiento de las normas, evaluar nuevas amenazas, gestionar la seguridad de los sistemas y formar a los empleados en buenas prácticas de ciberseguridad.

8.2 Oficiales de evaluación y seguimiento de cada proceso que deben realizar análisis y pruebas para detectar vulnerabilidades y dar cumplimiento de las políticas de seguridad, realizar seguimiento de proceso, monitorear continuamente las medidas de seguridad, verificar su efectividad, informar sobre desviaciones identificando debilidades, prevenir incidentes de seguridad para mantener un entorno seguro y confiable y asegurar la mejora continua.

9. METODOLOGÍA DE IMPLEMENTACIÓN

La implementación del presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se desarrollará conforme a los lineamientos establecidos en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, expedida por el Departamento Administrativo de la Función Pública (DAFP), en su versión vigente, la cual constituye el marco metodológico oficial para la gestión integral de los riesgos que puedan afectar el cumplimiento de los objetivos institucionales.

Dicha guía se encuentra alineada con el Modelo Integrado de Planeación y Gestión (MIPG) y establece directrices para la administración de riesgos en el sector público, incorporando la gestión de riesgos asociados a la seguridad digital, así como los riesgos de gestión, corrupción y fiscal, según las actualizaciones normativas aplicables.

El documento se fundamenta en el Modelo Integrado de Planeación y Gestión (MIPG) y aborda principalmente los riesgos de gestión, corrupción y seguridad digital, incorporando en sus versiones más recientes el riesgo fiscal. Asimismo, define la metodología para el diseño de controles, en concordancia con las actualizaciones de la política de administración del riesgo.

La metodología de gestión del riesgo contempla un proceso estructurado que incluye la identificación, el análisis, la evaluación, el tratamiento y el seguimiento de los riesgos. De igual manera, la guía proporciona orientaciones, pasos y herramientas para el diseño e implementación de controles internos y externos, con el fin de prevenir o mitigar los riesgos identificados.

En la alineación, la guía está integrada con el Modelo Integrado de Planeación y Gestión (MIPG) y el Marco Estándar de Control Interno, sirviendo como base para la política de administración de riesgos de las entidades.

La metodología por seguir de acuerdo a la Guía para la Administración del Riesgo y el diseño de controles en las entidades públicas es:

1. **Identificación de riesgos**: mediante el reconocimiento de amenazas, vulnerabilidades, activos de información y eventos que puedan afectar los procesos institucionales.

2. **Análisis y valoración de riesgos**: orientado a determinar la probabilidad de ocurrencia y el impacto potencial sobre la confidencialidad, integridad y disponibilidad de la información institucional.

3. **Evaluación de riesgos:** determinar el nivel de riesgo, estableciendo los niveles de aceptación y el mapa de calor. con el fin de establecer su nivel de criticidad y priorización para la adopción de medidas de control.

4. **Tratamiento de riesgos**: mediante la definición e implementación de acciones orientadas a mitigar, transferir, aceptar o evitar los riesgos identificados.

5. **Diseño de controles**: establecer los mecanismos para implementar los tratamientos definidos.

6. **Seguimiento y monitoreo:** a través de mecanismos de control, medición y mejora continua que permitan verificar la efectividad de las acciones implementadas y asegurar su actualización periódica.

Las tipologías de riesgo son:

1. **Riesgo de gestión**: relacionado con la planificación, ejecución y control de las operaciones de la institución.

2. **Riesgo de corrupción**: son aquellos que pueden afectar el cumplimiento de

los objetivos institucionales y el desarrollo normal de los procesos (planeación, ejecución, control, recursos, operación, etc.).

3. **Riesgo de seguridad digital**: Incluyen riesgos que afectan los activos de información, sistemas tecnológicos, redes, infraestructura digital y servicios institucionales, comprometiendo la confidencialidad, integridad y disponibilidad de la información.

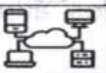
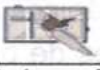
4. **Riesgo financiero:** Son aquellos que pueden generar afectación al patrimonio público, pérdidas económicas o impactos presupuestales, incluyendo fallas en la ejecución de recursos o decisiones con impacto financiero negativo.

5. **Riesgo de cumplimiento**: es el riesgo de que una entidad incurra en incumplimiento de normas, leyes, reglamentos, políticas internas o compromisos contractuales, lo cual puede generar consecuencias jurídicas, disciplinarias, fiscales, administrativas o reputacionales.

Los factores de riesgo corresponden a las fuentes, condiciones o agentes con capacidad inherente para generar eventos de riesgo. Estos pueden estar asociados a elementos físicos, mecánicos, tecnológicos, ambientales u organizacionales, así como a actos u omisiones de origen humano, que poseen el potencial de causar efectos adversos. La probabilidad de materialización del riesgo está determinada por la eficacia de los controles existentes y por las medidas de eliminación, mitigación o prevención implementadas.

Tabla 1 *Factores potenciales de riesgo en las organizaciones.*

FACTOR	DIFINICIÓN	GRAFICO	DESCRIPCIÓN
TALENTO HUMANO	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Falta de procedimientos
			Falta de capacitación en temas relacionados con el personal
			Hurto de activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)
TECNOLOGÍA	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos

FACTOR	DIFINICIÓN	GRAFICO	DESCRIPCIÓN
			Caída de aplicaciones
			Caída de redes
			Errores en programas
INFRAESTRUCURA	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
INFRAESTRUCURA	Eventos relacionados con la infraestructura física de la entidad.		Inundaciones
			Daños a activos fijos
EVENTO EXTERNO	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

Fuente: *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, Versión 7, del Departamento Administrativo de la Función Pública.*

Posteriormente, luego de haber identificado el contexto estratégico y entender el concepto de riesgos de seguridad de la información, se procede a realizar la definición de los controles. Para esto, los Líderes de Proceso deben analizar los siguientes procedimientos de seguridad de la información, con el fin de determinar cuáles son necesarios para reducir los riesgos en su gestión y que sirvan como guía para determinar los responsables, la periodicidad, propósito y evidencias del control para la seguridad de la información de la siguiente manera:

1. Procedimiento de gestión de activos de información.
2. Procedimiento control acceso áreas seguras.
3. Procedimiento de gestión de incidentes.
4. Procedimiento de recolección de evidencias digitales.
5. Procedimiento de criptografía.
6. Procedimiento de transferencia de información.
7. Procedimiento de seguridad en sistemas de información.
8. Procedimiento Derechos de propiedad intelectual.
9. Procedimiento de medios removibles.
10. Procedimiento de derechos de propiedad intelectual.

11. Procedimiento de evaluación del SGSI.
12. Procedimiento de gestión de cambios de infraestructura tecnológica.
13. Procedimiento de registro de bases de datos con datos personales ante la Superintendencia de Industria y Comercio.
14. Procedimiento de anonimización de datos personales estructurados.
15. Procedimiento de gestión de copias de respaldo.
16. Mantenimiento de Plan de Recuperación ante Desastres (DRP).
17. Procedimiento de datos abiertos.
18. Procedimiento de datos personales.

Los procedimientos[32] 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.

9.1 Gestión de Riesgos

La gestión de riesgos en materia de seguridad y privacidad de la información constituye un proceso esencial para garantizar la adecuada protección de los activos de información de las entidades públicas, así como para asegurar la continuidad de las operaciones institucionales y la protección de los datos bajo su custodia. Desde una perspectiva jurídica, la gestión de riesgos se fundamenta en los principios de legalidad, prevención, responsabilidad, planeación y eficiencia administrativa que orientan la función pública, y se materializa a través de la adopción de mecanismos sistemáticos que permitan identificar, analizar, evaluar y tratar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

Las entidades del Estado tienen el deber de implementar medidas administrativas, técnicas y organizativas orientadas a la protección de la información pública y de los datos personales que administran, así como a la prevención de incidentes que puedan comprometer la seguridad de los sistemas de información institucionales. En este contexto, la gestión de riesgos se convierte en una herramienta fundamental para anticipar posibles amenazas y vulnerabilidades, permitiendo adoptar decisiones informadas para su mitigación y control.

a. Tratamiento de riesgos

Representa una etapa fundamental de la gestión de riesgos, en la cual la entidad define e implementa las acciones orientadas a reducir, controlar, evitar

[32] 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

o asumir los riesgos previamente identificados y evaluados, consiste en buscar los niveles de riesgos aceptables para la organización. En primer lugar, es necesario determinar cuál será el nivel de tratamiento, por ello es necesario tener en cuenta que la eliminación total de un riesgo solamente es posible con la supresión de la actividad que lo provoca.

El tratamiento de riesgos implica la definición de estrategias y controles que permitan gestionar adecuadamente los riesgos identificados, teniendo en cuenta factores como la probabilidad de ocurrencia, el impacto potencial sobre los procesos institucionales y la capacidad de la entidad para implementar medidas de control. En este sentido, el tratamiento puede materializarse mediante diversas acciones, entre las cuales se encuentran la mitigación del riesgo mediante la implementación o fortalecimiento de controles de seguridad, la evitación del riesgo mediante la modificación de procesos o actividades que generen una exposición significativa, la transferencia del riesgo a terceros mediante mecanismos contractuales o de aseguramiento, o la aceptación del riesgo cuando su nivel residual se encuentra dentro de los niveles tolerables definidos por la entidad.

Asimismo, el proceso de tratamiento de riesgos debe integrarse con las políticas institucionales de seguridad y privacidad de la información, con los sistemas de gestión de seguridad digital y con los lineamientos de control interno, garantizando que las medidas adoptadas se encuentren alineadas con los objetivos estratégicos de la entidad y con el marco normativo vigente. De esta manera, el tratamiento de riesgos no se limita a la adopción de controles técnicos, sino que involucra también medidas organizacionales, administrativas, jurídicas y procedimentales que contribuyan a fortalecer la protección de los activos de información.

Entonces, dentro del tratamiento de los riesgos existen 5 medidas diferentes:

1. **Evitar el riesgo:** Consiste en adoptar decisiones que eliminen la actividad, proceso o condición que genera el riesgo identificado. Esta medida implica modificar o suspender determinadas operaciones cuando el nivel de riesgo resulta inaceptable o cuando no existen controles razonables que permitan reducirlo a niveles tolerables.

En el contexto de la seguridad de la información, la evitación del riesgo puede materializarse mediante la eliminación de sistemas obsoletos, la restricción de determinadas tecnologías que generen vulnerabilidades significativas, o la modificación de procesos que expongan información sensible sin los controles adecuados.

2. Mitigar o reducir el riesgo: Esta es la medida más común dentro del tratamiento de riesgos y consiste en implementar controles administrativos, técnicos o físicos orientados a disminuir la probabilidad de ocurrencia del riesgo o reducir el impacto que podría generar en caso de materializarse.

Entre las medidas de mitigación más utilizadas se encuentran:

- Implementación de controles de acceso a la información.
- Aplicación de políticas de seguridad de la información.
- Uso de mecanismos de cifrado y autenticación.
- Actualización y fortalecimiento de infraestructuras tecnológicas.
- Capacitación del personal en buenas prácticas de seguridad digital.
- Implementación de mecanismos de monitoreo y detección de incidentes.

Estas medidas permiten fortalecer la protección de la confidencialidad, integridad y disponibilidad de la información, que constituyen los pilares fundamentales de la seguridad de la información.

3. Transferir el riesgo: Implica trasladar total o parcialmente la responsabilidad del riesgo a un tercero, generalmente mediante mecanismos contractuales o instrumentos financieros. En el ámbito institucional, esto puede materializarse a través de contratos con proveedores especializados, acuerdos de nivel de servicio o la contratación de pólizas de seguros que cubran determinados eventos que puedan afectar los activos de información.

No obstante, es importante señalar que, aun cuando el riesgo sea transferido, la entidad conserva la responsabilidad de ejercer supervisión y control sobre las obligaciones del tercero.

4. Aceptar el riesgo: La aceptación del riesgo se presenta cuando, después de realizar el análisis correspondiente, la entidad determina que el nivel de riesgo residual se encuentra dentro de los niveles de tolerancia definidos institucionalmente o cuando el costo de implementar controles adicionales resulta desproporcionado frente al impacto potencial del riesgo.

En estos casos, el riesgo debe ser formalmente documentado y aprobado por la autoridad competente dentro de la entidad, dejando constancia de las razones que justifican su aceptación y de los mecanismos de seguimiento establecidos.

5. Monitorear y hacer seguimiento al riesgo: Aunque el seguimiento no constituye una medida de tratamiento en sentido estricto, sí forma parte esencial del proceso de gestión de riesgos. Consiste en evaluar periódicamente la efectividad de las medidas implementadas, verificar si el nivel de riesgo ha disminuido y determinar si es necesario adoptar nuevas acciones de control.

Este proceso permite mantener actualizada la gestión de riesgos frente a cambios tecnológicos, operacionales o normativos que puedan afectar la seguridad y privacidad de la información.

b. Monitoreo y revisión

Después de que las acciones para administrar los riesgos de seguridad de la información identificados en cada proceso sean diseñadas y validadas, es necesario establecer las actividades o estrategias para monitorearlos, teniendo en cuenta que estos nunca dejan de representar una amenaza para la integridad, disponibilidad y confidencialidad de la información institucional.

En consecuencia, el monitoreo es esencial para que cada proceso pueda asegurar que las acciones ejecutadas se estén llevando a cabo y así poder evaluar la eficacia de su implementación, realizando revisiones sobre la marcha para evitar situaciones que influyan en la aplicación de las acciones y en el avance de los indicadores.

El monitoreo de la administración de riesgos debe estar a cargo, en primera instancia, de los responsables de los procesos mediante la plataforma Suite Visión Empresarial.

c. Comunicación y consulta

En esta fase se establece la comunicación con las partes internas y externas que intervienen durante los pasos de la metodología de administración de riesgos, con el fin de que estos sean consultados sobre su capacidad para cumplir con las acciones establecidas para el tratamiento de los riesgos de seguridad de la información identificados. De esta manera, las partes involucradas son notificadas de sus responsabilidades frente a la gestión de los riesgos, y de los compromisos que deben cumplir en los tiempos establecidos, así como de los soportes que se deben generar para evidenciar el cumplimiento de las acciones asignadas.

Por último, es necesario que los responsables de la gestión de riesgos de

seguridad de la información en cada proceso, continúen trabajando en la revisión, aprobación e implementación de controles de seguridad de la información, orientados a reducir los riesgos de seguridad de la información.

d. Clasificación de los Riesgos

La clasificación de los riesgos dentro del **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información** permite priorizar aquellos riesgos que representan una mayor amenaza para la entidad, facilitando la asignación eficiente de recursos y la implementación de controles adecuados. Asimismo, esta clasificación constituye un instrumento de apoyo para el proceso de toma de decisiones institucionales, al proporcionar una visión estructurada de los riesgos que pueden afectar la seguridad, disponibilidad, integridad y confidencialidad de la información.

***Tabla 2** Clasificación de los riesgos*

Fallas Tecnológicas	✓ Limitación de redes, datos y comunicaciones, cobertura y disponibilidad de servicios tecnológicos, mantenimiento y soporte en unidades militares.
Seguridad de la Información	✓ Desconocimiento y/o no idoneidad del personal que desarrolla las responsabilidades de gestión y control de seguridad en los segmentos de red que permitan generar cultura de seguridad con la información digital.
	✓ Falta de aplicación o difusión de los controles de acceso en seguridad de la información que afectan la confidencialidad de la información del Ejército Nacional.
	✓ Fallas en los sistemas de seguridad digital institucionales.
	✓ Fallas en los sistemas de información y/o equipos del componente C5 institucionales.
Corrupción	✓ Desviación de los recursos asignados al componente C5.
Legitimidad	✓ Desactualización de la normatividad de los procesos, procedimientos, formatos y/o directivas.

***Fuente:** elaboración propia.*

La clasificación más utilizada dentro de los planes de tratamiento de riesgos consiste en establecer el **nivel de riesgo**, el cual resulta de la combinación entre la **probabilidad de ocurrencia del evento** y el **impacto que generaría en la entidad**. A partir de esta valoración se suelen definir categorías como:

- **Riesgo bajo:** requiere monitoreo y controles básicos.
- **Riesgo moderado:** requiere implementación de controles de mitigación.

- **Riesgo alto:** exige acciones inmediatas de tratamiento y fortalecimiento de controles.
- **Riesgo crítico:** requiere intervención prioritaria y medidas estrictas de control.

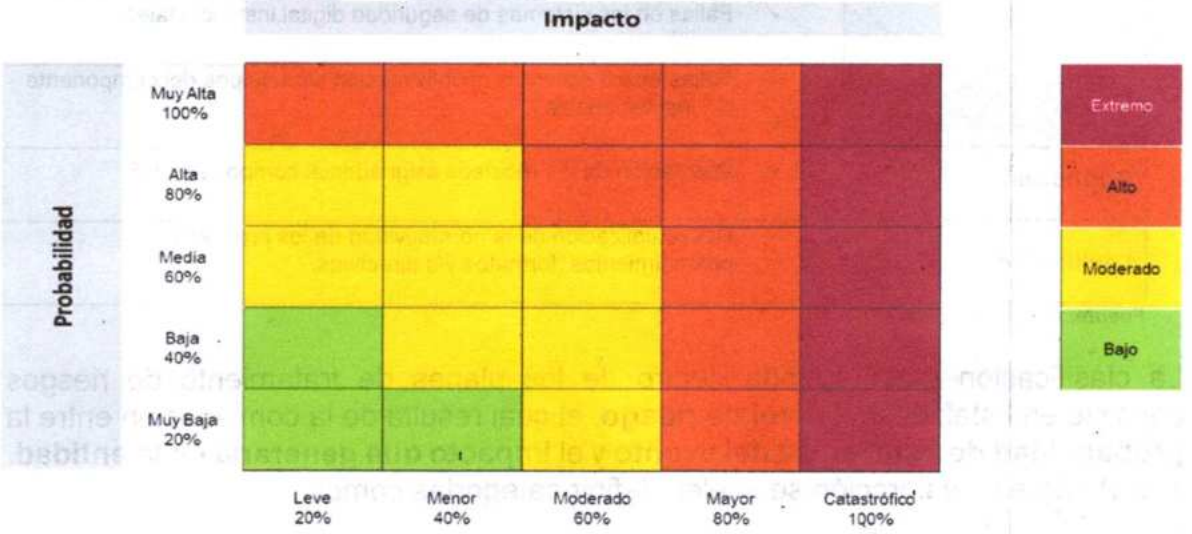
e. Medición del Riesgo

La medición de los riesgos permite a la entidad establecer un criterio técnico y objetivo para la administración de los riesgos asociados a la seguridad y privacidad de la información, facilitando la priorización de acciones de tratamiento y la asignación eficiente de recursos. Asimismo, fortalece la capacidad institucional para prevenir incidentes de seguridad, proteger los activos de información y garantizar la continuidad de las funciones misionales del Estado.

Una vez se realicen los reportes de cumplimiento de los planes de tratamiento y controles, los responsables del proceso de Seguridad y Privacidad de la Información, Gestión de Tecnologías C5 (Comando, Control, Computación, Ciberdefensa, Comunicaciones), realizan la revisión y validación de esta información, con el fin de reportar la medición de la gestión del riesgo a través del indicador que tiene como propósito medir el nivel de implementación de los controles de los riesgos.

Análisis preliminar (riesgo inherente): se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.

***Ilustración 3** Matriz de calor (análisis de severidad del riesgo)*



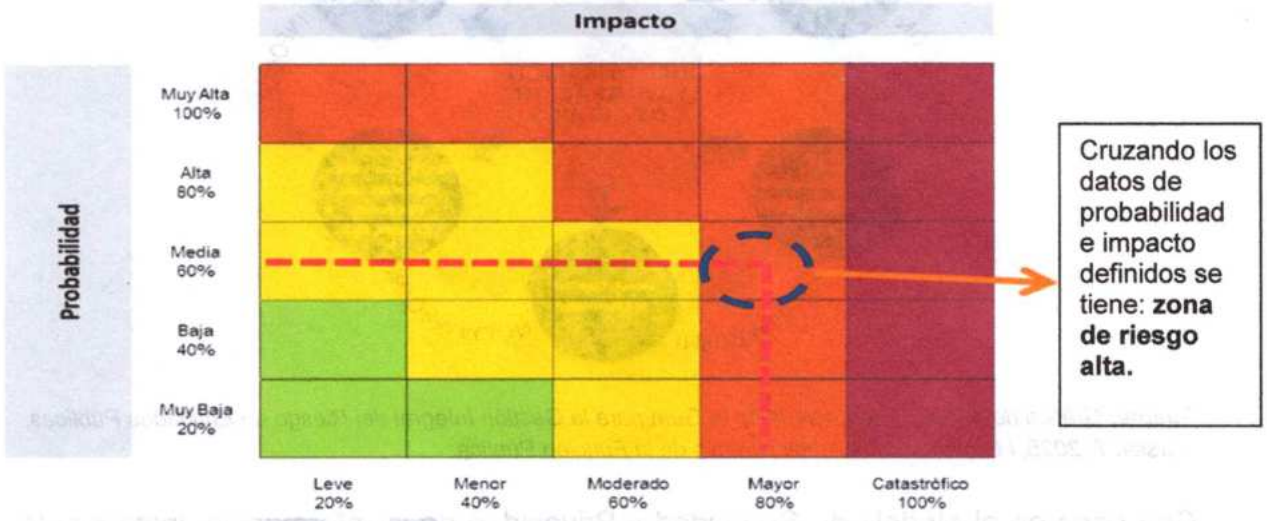
***Fuente**: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, Versión 6, del Departamento Administrativo de la Función Pública.*

Generalmente, la probabilidad se clasifica en niveles cualitativos o cuantitativos, tales como:

- **Muy baja:** el evento es poco probable de ocurrir y existen controles sólidos que reducen significativamente su posibilidad.
- **Baja:** el evento podría ocurrir en circunstancias excepcionales.
- **Media:** el evento tiene una probabilidad moderada de ocurrir.
- **Alta:** el evento es probable que ocurra en determinadas condiciones.
- **Muy alta:** el evento tiene una alta probabilidad de ocurrir debido a debilidades significativas en los controles o a una alta exposición al riesgo.

Aplicando la matriz de calor tenemos:

Ilustración 4 *Zonas de riesgo*



Fuente*: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, Versión 6, del Departamento Administrativo de la Función Pública.*

Los resultados de la medición deben quedar formalmente registrados dentro del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, indicando para cada riesgo identificado:

- el activo de información afectado,
- la amenaza o vulnerabilidad asociada,
- el nivel de probabilidad,
- el nivel de impacto,
- el nivel de riesgo resultante, y
- las medidas de tratamiento definidas.

En atención a lo anteriormente dicho a continuación, se desarrollan los pasos necesarios para la identificación y tratamiento de los riesgos asociados a la disponibilidad, integridad y confidencialidad de los activos de información:[33]
En la siguiente gráfica se muestran los pasos para la identificación y valoración de activos para la seguridad de la información:

Ilustración 5 *Pasos para la identificación de riesgos*

Fuente: *Gráfica de MinTIC referenciada en la Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, 2025, I Departamento Administrativo de la Función Pública.*

Con base en el Modelo de Seguridad y Privacidad de la Información, instrumento desarrollado por el Ministerio de Tecnologías de la Información y las Comunicaciones, el cual establece los lineamientos para diseñar, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información conforme a normas y estándares internacionales de buenas prácticas, se orienta la gestión institucional en esta materia.

De igual manera, mediante la Guía para la Gestión Integral del Riesgo en Entidades Públicas, expedida por el Departamento Administrativo de la Función Pública, se estructuran los procesos de identificación, análisis, tratamiento y seguimiento de los riesgos asociados a la seguridad de la información.

[33] Función Pública, Guía para la Gestión Integral del riesgo en Entidades Públicas, versión 7, 2025.

En este marco, para el Ejército Nacional de Colombia se diseñan y establecen los lineamientos y mecanismos necesarios para la ejecución y el seguimiento efectivo de la gestión de riesgos en seguridad de la información, garantizando su adecuada implementación y control institucional.

Para los riesgos que tienen como objetivo orientar al sector público en la implementación de un proceso de gestión de riesgos de seguridad de la información, que permita incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en las entidades y que se deben desarrollar los pasos de identificación y tratamiento de los riesgos asociados a la Disponibilidad, Integridad y Confidencialidad de los activos de información que permitan cumplir con la misión y alcanzar la visión institucional, siendo estos pasos los siguientes:

1. Identificación y descripción de riesgos de seguridad de la información.

   - ✓ Identificación de los riesgos clave y asociación de estos frente a los objetivos previamente identificados.
   - ✓ Identificación de áreas de impacto.
   - ✓ Identificación de áreas de factores de riesgo.
   - ✓ Descripción del riesgo.
   - ✓ Descripción del riesgo.

2. Análisis del Riesgo Inherente.

   - ✓ Determinar la **probabilidad** (frecuencia, %probabilidad inherente, **probabilidad inherente** (muy baja-20%, baja-40%, media-60%, altsa-80%, muy alta-100%).
   - ✓ Determinar el **impacto** (%Impacto Inherente, impacto inherente), nivel del impacto (leve-20%, menor-40%, moderado-60%, mayor-80%, catastrófico-100%).
   - ✓ Análisis de severidad (probabilidad (muy baja-20%, baja-40%, media-60%, alta-80%, muy alta-100%), impacto (leve-20%, menor-40%, moderado-60%, mayor-80%, catastrófico 100%)

3. Diseño y Análisis de Controles.

   - ✓ Estructura para la Descripción del Control (N°. control, Anexo A de la Norma ISO 27001:2022, descripción del control).
   - ✓ Valoración de Controles, Afectación (probabilidad, impacto, atributos).

4. Valoración de Riesgo Residual.

Se debe en esta etapa revisar la efectividad de los controles, teniendo en cuenta la aplicación de controles para establecer el riesgo residual:

1. Probabilidad residual.
2. % de probabilidad residual.
3. Impacto residual.
4. % de impacto residual.
5. zona de riesgo final.

Se debe elaborar un plan de acción con responsables, fecha de implementación, estado y elaborar la matriz de riesgos de seguridad de la información para los análisis requeridos.

10. ACTIVIDADES PLAN DE ACCIÓN Y SEGUIMIENTO

Tabla 3 *Cronograma de actividades plan de acción.*

ACTIVIDADES	ENTREGABLE	RESPONSABLE	PERIODICIDAD		
Actualizar el uso contexto estratégico e identificación de los riesgos	Contexto Estratégico Actualizado	Encargados Seguimiento y Evaluación de Calidad para el Sistema de Seguridad de la Información en CEDE6	Anual	1/01/2026	30/11/2026
Definir los Riesgos	Formato FO-CEDE5-DIGEC-487 Diligenciado				
Aprobar los riesgos del Proceso de "Gestión de tecnologías y Sistemas de Información C5"	Oficio de aprobación				
Socializar las acciones para el tratamiento de los riesgos.	Acta de reunión de Socialización				

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

Nota: *Los Líderes y Oficiales de Evaluación y Seguimiento de cada proceso son responsables del cumplimiento de las actividades establecidas.*

Tabla 4 *Actividades de Seguimiento e identificación riesgos seguridad de la información.*

Seguimiento e identificación de Riesgos				
ACTIVIDADES	TAREAS	RESPONSABLE DE LA TAREA	FECHA INICIO	FECHA FINAL
Sensibilización	Socialización gestión de riesgos de seguridad y privacidad de la información, seguridad digital.	Encargados Seguimiento y Evaluación de Calidad para el Sistema de	01/09/2026	30/11/2026
Identificación de Riesgos de Seguridad y	Identificación, análisis y evaluación de			

Privacidad de la Información, Seguridad Digital y continuidad de la Operación	riesgos - seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	Seguridad de la Información	
	Realimentación, revisión y verificación de los riesgos identificados (Ajustes).		
Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento.		
Seguimiento Fase de Tratamiento	Seguimiento estado plan de tratamiento de riesgos identificados y verificación de evidencias.		
Evaluación de riesgos residuales	Evaluación de riesgos residuales.		
Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales.		
	Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo a los cambios solicitados.		
Monitoreo y Revisión	Generación, presentación y reporte de indicadores.		

Fuente: *Formato diligenciado anualmente donde se incluyen las actividades del Plan de Acción CEDE6 (FO-CEDE5-DIPLE-1852)*

Tabla 5 *Gestión de riesgos 2026*

Gestión de Riesgos 2026 Periodicidad Trimestral /Semestral/Anual
➢ Posibilidad de afectación reputacional por las fallas en los sistemas de seguridad digital institucionales debido a la inadecuada aplicación de los procedimientos para la gestión de acceso, copias de respaldo y el seguimiento a la instalación de agentes de seguridad en los equipos que afectan la **integridad de los activos de información.**
➢ Posibilidad de afectación reputacional por falta de aplicación o difusión de los controles de acceso en seguridad de la información debido al inadecuado cumplimiento de los protocolos de seguridad y reserva de la información, que afectan la **confidencialidad de la información del Ejército Nacional**
➢ Posibilidad de afectación reputacional por las fallas en los sistemas de información y/o equipos del componente C5 institucionales, debido al inadecuado control y verificación de estos, que afectan la **disponibilidad de la información del Ejército Nacional.**
➢ Posibilidad de afectación reputacional por **corrupción** en el desvío de material (Cómputo, Equipos de comunicaciones, accesorios, repuestos) del componente c5 del Ejercito Nacional **a unidades que no estaban relacionadas en el plan de distribución. a causa de fallas en el seguimiento y control de la asignación de bienes.**

Fuente: *Formato diligenciado anualmente donde se incluyen las actividades del Plan de Acción CEDE6 (FO-CEDE5-DIGEC-487, FO-CEDE5-DIGEC-1975).*

11. SEGUIMIENTO Y EVALUACIÓN DEL PRESENTE PLAN

Con la finalidad de valorar el impacto del presente Plan y del funcionamiento de la gestión de riesgos, es pertinente evaluar los siguientes indicadores:

Tabla 6 *Indicador eficiencia acciones control de riesgos.*

Nombre del Indicador: Eficiencia Acciones de Control Riesgos	
Meta: *Verificar el 100 % de cumplimiento de actividades de control establecidas para la gestión de los riesgos de seguridad de la información identificados para la vigencia 2026.*	
Meta año anterior: *N/A*	**Meta:***100 %*
Tipo de indicador: *eficiencia (EFC)*	**Formula del indicador:** *(V1/V2) x100*
Variable 1 – V1: *total de actividades ejecutadas para la gestión de los riesgos de seguridad de la información vigencia 2026.* Fuente de información: las actividades a cumplir corresponden a las definidas en el formato FO-CEDE5-DIGEC-487, para los riesgos de seguridad de la información vigencia 2026 y se monitorean por medio de la Suite Visión Empresarial.	**Variable 2 – V2:** *número de actividades de control establecidas en cada uno de los riesgos de seguridad de la información 2026.* Es la planeación de las actividades propuestas para la gestión de los riesgos de seguridad de la información de la vigencia 2026.
Evaluación: *trimestral*	**Tendencia:** *estable*

Fuente: *elaboración propia*

12. ENTREGABLES

1. Actas de reunión o informes como soporte de la gestión de riesgos de seguridad de la información del año 2026.

2. Formato FO-CEDE5-DIGEC-487 diligenciado.

13. NORMATIVIDAD DE REFERENCIA

1. Constitución Política de Colombia (1991).[34]
2. 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".
3. Ley 1581 del 17 de octubre de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales".
4 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".
5. 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.
6. 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".
7. 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".
8. 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".
9. 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

[34] 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".

la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones".

10. Resolución 007722 del 25 de octubre de 2021, "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", emitido por el Ejército Nacional.
11. Resolución 463 del 09 de febrero de 2022, "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones".
12. Reglamento Generador de Fuerza del Ejército Nacional RGE 4-0.1 (RGE), "Gestión Documental para el Ejército Nacional".
13. Manual Operativo Modelo Integrado de Planeación y Gestión (MIPG), versión 6 de 2024.
13. Directiva Permanente 7870 del 26 de diciembre de 2022, "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", emitido por el Ministerio de Defensa Nacional.
14. 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.
15. Directiva Permanente 00200 del 27 de diciembre de 2017, Ejército Nacional, "Computación", la que la modifique, aclare o adicione.
16. 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.
17. Directiva Permanente N°2025228010640103 del 16 de junio de 2025,"Lineamientos para el desarrollo de la Política General de Seguridad de la información en el Ejército Nacional".
18. Directiva Permanente 03 del 23 de enero de 2019, Ministerio de Defensa Nacional, "Lineamientos para la definición de la Política de Tratamiento de

Datos Personales en el Ministerio de Defensa".

19. 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.
20. Documento CONPES 3854 del 11 de abril de 2016, "Política Nacional de Seguridad Digital".
21. Documento CONPES 3995 del 1 de julio de 2020, "Política Nacional de Confianza y Seguridad Digital".
22. Documento CONPES 4144 14 de febrero de 2025, "Política Nacional de Inteligencia Artificial".
23. Resolución 02277 de 2025, "Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia".
24. Plan Estratégico Institucional 2022 - 2026 (PEI), "Hombres y Mujeres de Honor al Servicio de la Nación" del Departamento de Planeación CEDE5.
25. Guía metodológica para la administración de riesgos 2022 del Departamento de Planeación CEDE5.

Firma,

3960

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