PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN "PESI" – VIGENCIA 2025.

ELABORÓ	REVISÓ	APROBÓ
NOMBRE: Ing. Deiby Leandro Alvarado Rodríguez.	**NOMBRE:** Ing. Ricardo Valenzuela Díaz.	**NOMBRE:** Abog. Martha Eugenia Cortés Baquero.
CARGO: Profesional Defensa – Seguridad de la Información.	**CARGO:** Líder Proceso Gestión de Tecnologías de la Información y las Comunicaciones.	**CARGO:** Jefe de la Oficina Asesora Jurídica, encargada de la Funciones del Despacho de la Dirección General de la Agencia Logística de las Fuerzas Militares.
FIRMA:	**FIRMA:**	**FIRMA Y FECHA DE APROBACIÓN:** 23 01 2025

TABLA DE CONTENIDO

1. GENERALIDADES

La Agencia Logística de las Fuerzas Militares (ALFM) reconoce que la información es un recurso estratégico fundamental para el cumplimiento de su misión y la consecución de sus objetivos institucionales. Este activo, en cualquiera de sus formas de uso, procesamiento o almacenamiento, debe ser protegido frente a amenazas internas y externas para garantizar su confidencialidad, integridad y disponibilidad. Asimismo, entiende que los sistemas de información son el soporte principal de sus procesos operativos y administrativos, lo que demanda estrategias sólidas para su control y protección.

Para lograrlo, la ALFM ha adoptado metodologías específicas que permiten identificar, valorar y gestionar los riesgos relacionados con sus activos de información, asegurando una protección proactiva. Este enfoque está articulado a través del Modelo de Seguridad y Privacidad de la Información (MSPI), que establece políticas, procedimientos y controles alineados con los objetivos estratégicos de la entidad. Además, dichos controles se supervisan continuamente mediante indicadores de gestión y revisiones periódicas que facilitan la mejora continua del modelo.

En cumplimiento de las directrices gubernamentales y la Política de Gobierno Digital, la implementación del MSPI está respaldada por normativas como el Decreto 612 de 2018 y la Resolución 500 de 2021, entre otras. Estas normativas establecen el marco para fortalecer la capacidad institucional en la gestión de la seguridad y privacidad de la información, permitiendo a la entidad responder de manera efectiva a los desafíos actuales y futuros en esta materia.

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) refleja la visión de la ALFM hacia la transformación digital y el uso responsable de las Tecnologías de la Información y las Comunicaciones (TIC). Este plan no solo busca garantizar el cumplimiento normativo, sino también generar confianza en el uso de la tecnología mediante proyectos que optimizan los sistemas de información, mejoran la infraestructura tecnológica y fortalecen la capacidad de respuesta ante riesgos y amenazas. Con esta perspectiva, la ALFM asegura que sus iniciativas contribuyan de manera directa al logro de sus objetivos institucionales y a la satisfacción de las necesidades de sus partes interesadas.

El presente plan es presentado al Comité Institucional de Gestión y Desempeño, para someterlo a su respectiva aprobación y publicación en la página web institucional; conforme al Decreto 612 de 2018.

2. REFERENCIA NORMATIVA

Conforme con lo establecido en la normatividad vigente el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del MSPI en la entidad.

Constitución Política	Aplicación de los artículos 15, 209 y 269.

de la República de Colombia.	
Ley 594 de 2000 (julio 14).	Por la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
Ley 599 de 2000 (julio 24).	Código Penal Colombiano.
Ley 1221 de 2008 (julio 16).	Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
Ley 1266 de 2008 (diciembre 31).	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273 de 2009 (enero 05).	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.
CONPES 3701 de 2011 (julio 14).	Lineamientos de política para ciberseguridad y ciberdefensa.
Ley 1581 de 2012 (octubre 17).	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2364 de 2012 (noviembre 22).	Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Decreto 2609 de 2012 (diciembre 14).	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.
Directiva Permanente Ministerio Defensa No. 913 de 2013 (abril 19).	Guías y procedimientos en tecnología de información y comunicaciones para el Sector Defensa.
Decreto 1377 de 2013 (junio 27).	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 886 de 2014 (mayo 13).	Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Ley 1712 de 2014 (marzo 06).	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Directiva Permanente Ministerio de Defensa No. 018 de 2014 (junio 19).	Políticas de seguridad de la información para el Sector Defensa.
Decreto 2573 de 2014 (diciembre 12).	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la

	Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 103 de 2015 (enero 20).	Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1078 de 2015 (mayo 26).	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
CONPES 3854 de 2016 (abril 11).	Política Nacional de Seguridad digital.
Decreto 728 de 2017 (mayo 05).	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Decreto 1413 de 2017 (agosto 25).	Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título 111 de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
CONPES 3920 de 2018 (abril 17).	Política nacional de explotación de datos (BIG DATA).
Decreto 1008 del 2018 (junio 14).	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.
Ley 1915 de 2018 (julio 12).	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Decreto 612 de 2018 (abril 04).	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.
Directiva Presidencial No. 02 de 2019 (abril 02).	Simplificación de la interacción digital entre los ciudadanos y el estado.
Decreto 2106 de 2019.	Establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
Ley 1952 de 2019.	Por medio de la cual se expide el código general disciplinario.
Decreto 620 de 2020 (mayo 2).	Por el cual se subroga el título 17 de la parte 2 del libro 2 del decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la ley 1437 de 2011, los

	literales e, j y literal a del parágrafo 2 del artículo 45 de la ley 1753 de 2015, el numeral 3 del artículo 147 de la ley 1955 de 2019, y el artículo 9 del decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
CONPES 3995 de 2020 (julio 01).	Nacional de confianza y seguridad Digital.
Resolución 1519 de 2020 (agosto 24).	Por la cual se definen los estándares y directrices para publicar la información señalada en la ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Ley 2052 de 2020 (agosto 25).	Por medio de la cual se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial y a los particulares que cumplan funciones públicas y/o administrativas, en relación con la racionalización de trámites y se dictan otras disposiciones.
Decreto 045 de 2021 (enero 15).	Por el cual se derogan el Decreto 704 de 2018 y el artículo 1.1.2.3. del Decreto 1078 de 2015, Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Resolución 413 de 2021 (marzo 01).	Por la cual define el uso de las tecnologías en la nube para el sector defensa y se dictan otras disposiciones.
Resolución 500 de 2021 (marzo 10).	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.
Directiva Presidencial No. 03 de 2021 (marzo 15).	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
Decreto 377 de 2021 (abril 9).	Por el cual se subroga el título 1 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, para reglamentar el Registro Único de TIC y se dictan otras disposiciones
Decreto 88 de 2022 (enero 24).	Por el cual se adiciona el Titulo 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.
Resolución 0463 de 2022 (febrero 09).	Por el cual se define el uso de Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones.
Resolución 000460 de 2022 (febrero 15).	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.
Directiva Presidencial No. 02 de 2022 (febrero 24).	Por medio del cual se efectúa reiteración de la política pública en materia de seguridad digital.
Decreto 338 de 2022 (marzo 8).	Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
Resolución 000746 de 2022 (marzo 11).	Por el cual se fortalece el modelo de seguridad y privacidad de la información y se definen lineamientos adicionales a los establecidos en la resolución no. 500 de 2021.
Decreto 767 de 2022 (mayo 16).	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.
Decreto 1263 de 2022 (julio 2022).	Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública.
Resolución 7870 de 2022 (diciembre 26).	Por la cual se emite y adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa, y se dictan otras disposiciones.
Norma ISO/IEC 27001:2022.	Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.
Ley 2294 de 2023 (mayo 19).	Por el cual se expide el plan nacional de desarrollo 2022 – 2026 "Colombia potencia mundial de vida".
Manual integrado de gestión de 2024 (octubre 3).	Manual integrado de gestión, código: GI-MA-02, versión No. 22.

3. OBJETIVO DEL PLAN

Fortalecer las estrategias de seguridad y privacidad de la información mediante la evolución del Modelo de Seguridad y Privacidad de la Información (MSPI), priorizando la mejora continua en la protección de la integridad, confidencialidad y disponibilidad de los activos de información. Esto incluye garantizar el cumplimiento de las normativas vigentes, promover

la confianza en la gestión de datos y robustecer la infraestructura tecnológica de la entidad para enfrentar los desafíos del entorno digital.

3.1. OBJETIVOS ESPECIFICOS

Establecer y consolidar la estrategia de seguridad digital en la ALFM, alineada con el Modelo de Seguridad y Privacidad de la Información (MSPI) y las normativas vigentes, para fortalecer la resiliencia frente a amenazas cibernéticas.

Implementar medidas proactivas para garantizar la protección de la información en la ALFM, mitigando riesgos asociados a incidentes, accesos no autorizados, filtraciones de datos y ataques cibernéticos.

Fomentar la mejora continua en la estrategia de seguridad de la información mediante revisiones periódicas, implementación de controles, y evaluación del desempeño de las políticas definidas en el MSPI.

Asegurar la disponibilidad, continuidad y eficiencia de los servicios tecnológicos, minimizando interrupciones operativas a través de una gestión efectiva de infraestructura y procesos.

Fortalecer los controles de seguridad y privacidad de la información en los procesos y servicios de TI, garantizando la confidencialidad, integridad y disponibilidad de los activos de información y fomentando la confianza de las partes interesadas.

4. ALCANCE

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) abarca la totalidad de la Agencia Logística de las Fuerzas Militares (ALFM), comprendiendo todas sus sedes, regionales, dependencias operativas, administrativas y de apoyo a nivel nacional. Este plan tiene como propósito establecer e implementar medidas de seguridad y control destinadas a proteger la confidencialidad, integridad y disponibilidad de los activos de información en cada uno de los niveles operativos de la entidad; garantizando la continuidad de los procesos institucionales y la alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI), así como con las normativas legales y regulatorias vigentes.

El PESI se concibe como una herramienta dinámica y en permanente actualización, que permite la adopción de nuevas tecnologías de ciberseguridad, el fortalecimiento de la capacidad de respuesta ante amenazas emergentes y la incorporación de lecciones aprendidas de ciclos anteriores. Esta perspectiva flexible garantiza la adaptación a los cambios del entorno digital, con un enfoque proactivo en la protección de los activos críticos de información.

5. CUERPO DEL PLAN

5.1. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La Agencia Logística de las Fuerzas Militares (ALFM) reconoce que, como entidad pública, está cada vez más expuesta a incidentes de seguridad digital que podrían comprometer su funcionamiento y afectar la prestación de servicios a las partes interesadas. En respuesta a estos desafíos, se ha adoptado los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), los cuales promueven políticas, planes, programas y proyectos enfocados en el uso y la apropiación de las TIC. Esto permite establecer directrices claras para generar confianza en el entorno digital, garantizando un aprovechamiento seguro y eficiente de las tecnologías de la información y las comunicaciones.

En este contexto, el MinTIC ha desarrollado el Modelo de Seguridad y Privacidad de la Información (MSPI), que define los lineamientos para implementar una estrategia integral de seguridad digital. Su objetivo principal es formalizar, al interior de las entidades, un Sistema de Gestión de Seguridad de la Información (SGSI) y una estructura de seguridad digital basada en el ciclo PHVA (Planear, Hacer, Verificar y Actuar). Este enfoque considera los requerimientos legales, técnicos, normativos, reglamentarios y operativos necesarios para garantizar la protección de los activos de información.

El modelo se estructura en cinco fases fundamentales, diseñadas para gestionar y mantener de manera adecuada la seguridad y privacidad de la información, asegurando su alineación con las mejores prácticas y el marco normativo vigente.

5.1.1. FASE 1. Diagnóstico.

La primera fase del Modelo de Seguridad y Privacidad de la Información (MSPI) consiste en realizar un diagnóstico inicial o análisis GAP, cuyo objetivo es identificar el estado actual de la entidad frente a los lineamientos del modelo. Este análisis permite detectar brechas normativas y técnicas, evaluando aspectos como la gestión de riesgos, las políticas de seguridad, la protección de activos de información y la madurez del Sistema de Gestión de Seguridad de la Información (SGSI). Los resultados obtenidos sirven como base para la fase de planificación, facilitando la definición de estrategias y acciones correctivas, y se actualizan durante la evaluación de desempeño para medir avances y asegurar que el modelo evolucione según las necesidades institucionales. Esta etapa es clave para garantizar una implementación eficiente y alineada con las normativas vigentes.

5.1.2. FASE 2. Planificación.

En esta fase, se determinan las necesidades y objetivos estratégicos relacionados con la seguridad y privacidad de la información, considerando el mapa de procesos, el tamaño de la entidad y su contexto interno y externo. Esto incluye el análisis de prioridades

institucionales, requerimientos normativos, riesgos identificados en el diagnóstico y expectativas de las partes interesadas. Un componente clave es la Valoración y Tratamiento de Riesgos, que establece estrategias para mitigar, transferir, aceptar o evitar los riesgos, mediante la clasificación de activos de información, priorización de riesgos y definición de controles. Asimismo, se determinan los recursos necesarios, el cronograma de implementación y los indicadores clave de desempeño (KPI) para monitorear avances, asegurando que las actividades estén alineadas con los objetivos estratégicos. Esta fase es crucial, ya que define la base para el éxito del modelo, garantizando la integridad, confidencialidad y disponibilidad de los activos de información en un contexto normativo y organizacional alineado.

5.1.3. FASE 3. Operación.

En esta fase, se implementan los controles definidos en la planificación para mitigar los riesgos de seguridad de la información, reduciendo el impacto o la probabilidad de incidentes. Estos controles incluyen medidas técnicas, como firewalls, cifrado y autenticación multifactorial, y administrativas, como políticas, procedimientos y programas de capacitación. También se establecen procedimientos para gestionar incidentes de seguridad, abarcando su detección, análisis, respuesta y documentación, lo que refuerza la capacidad preventiva de la entidad. Paralelamente, se promueve una cultura de seguridad mediante sensibilización y formación del personal, y se asegura la integración de los controles con la infraestructura tecnológica existente a través de pruebas que validen su eficacia. Esta fase traduce las estrategias en acciones concretas para proteger los activos de información y garantizar la continuidad operativa frente a amenazas emergentes.

5.1.4. FASE 4. Evaluación de desempeño.

En esta fase, se lleva a cabo una evaluación exhaustiva del estado de adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) a través de auditorías internas y el análisis de los indicadores definidos en la planificación. Estas auditorías permiten verificar la efectividad de los controles implementados, identificar desviaciones y evaluar el grado de cumplimiento de los objetivos estratégicos y normativos. Además, el seguimiento de indicadores clave de desempeño (KPI) facilita la medición de avances, el análisis de tendencias y la identificación de áreas de mejora. Los resultados de esta fase no solo garantizan la alineación continua con el MSPI, sino que también proporcionan insumos clave para alimentar el proceso de mejora continua, asegurando que la seguridad de la información se gestione de manera eficiente y en línea con las necesidades institucionales.

5.1.5. FASE 5. Mejoramiento continuo.

En esta fase, se establecen procedimientos sistemáticos para identificar desviaciones en los controles y reglas definidos en el Modelo de Seguridad y Privacidad de la Información (MSPI), con el fin de detectar tempranamente cualquier fallo en su implementación. Cuando se identifican desviaciones, se planifican y ejecutan acciones correctivas y preventivas para solucionar los problemas y evitar su recurrencia. Este proceso incluye el análisis de las

causas raíz de los incidentes, la actualización de controles y políticas cuando sea necesario, y la implementación de nuevas estrategias para fortalecer la seguridad y privacidad de la información. Los resultados de estas actividades alimentan un ciclo continuo de mejora, garantizando que el modelo evolucione de acuerdo con los cambios en el entorno normativo, tecnológico y de riesgos, asegurando que la entidad mantenga altos estándares de protección en todos sus procesos.

En la Agencia Logística de las Fuerzas Militares (ALFM), las fases del Modelo de Seguridad y Privacidad de la Información (MSPI) se han trabajado de manera continua a lo largo de las vigencias, permitiendo una implementación gradual y progresiva. Este enfoque ha asegurado el cumplimiento de la normatividad vigente y la alineación con las necesidades específicas de la entidad. A continuación, se presentan los resultados del autodiagnóstico realizado durante la vigencia 2024, el cual refleja el estado actual de la implementación y los avances alcanzados en materia de seguridad y privacidad de la información.

Como se evidencia en la evaluación del avance del ciclo de funcionamiento del modelo PHVA (Planificar, Hacer, Verificar y Actuar) para el Modelo de Seguridad y Privacidad de la Información (MSPI), la entidad ha logrado un cumplimiento del 71% en la implementación del modelo operativo. El 29% restante se encuentra en proceso de gestión y continuará desarrollándose para alcanzar las fases de Efectivo y Gestionado, asegurando la consolidación del modelo en todos los niveles de la entidad.

Es importante resaltar que, dada la naturaleza dinámica de la seguridad de la información, la entidad se mantiene atenta a las actualizaciones normativas que emita el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). En particular, se considera relevante la incorporación de los cambios relacionados con la actualización de la ISO/IEC 27001:2022, incluyendo la estructuración de su Anexo A: Referencia de controles de seguridad de la información. Estos nuevos lineamientos permitirán ajustar y fortalecer las estrategias de seguridad, garantizando que se alineen con las mejores prácticas internacionales y las necesidades institucionales.

Tabla 1.
Avance ciclo de funcionamiento del modelo de operación (PHVA).

AVANCE PHVA		
COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
Planificación	34%	40%
Implementación	17%	20%
Evaluación de desempeño	17%	20%
Mejora continua	18%	20%
TOTAL	**86%**	**100%**

Nota. Avance implementación ciclo PHVA – Instrumento de identificación de la línea base de seguridad, autodiagnóstico Modelo de Seguridad y Privacidad de la Información – MSPI, ejecución vigencia (2024).

Tabla 2.
Evaluación de efectividad de controles.

No.	DOMINIO	Calificación Actual	Calificación Objetivo	Efectividad del control
A.5	Políticas de Seguridad de la Información	100	100	Optimizado
A.6	Organización de la Seguridad de la Información	75	100	Gestionado
A.7	Seguridad de los Recursos Humanos	87	100	Optimizado
A.8	Gestión de Activos	69	100	Gestionado
A.9	Control de acceso	67	100	Gestionado
A.10	Criptografía	40	100	Repetible
A.11	Seguridad física y del entorno	66	100	Gestionado
A.12	Seguridad de las Operaciones	74	100	Gestionado
A.13	Seguridad de las Comunicaciones	78	100	Gestionado
A.14	Adquisición, Desarrollo y Mantenimiento de Sistemas	59	100	Efectivo
A.15	Relación con los proveedores	60	100	Efectivo
A.16	Gestión de Incidentes de Seguridad de la Información	80	100	Gestionado
A.17	Aspectos de seguridad de la información de la Gestión de la Continuidad del Negocio	74	100	Gestionado
A.18	Cumplimiento	71,5	100	Gestionado
PROMEDIO EVALUACIÓN DE CONTROLES		**71**	**100**	**GESTIONADO**

Nota. Avance evaluación de efectividad de controles – Instrumento de identificación de la línea base de seguridad, autodiagnóstico Modelo de Seguridad y Privacidad de la Información – MSPI, ejecución vigencia (2024).

Con base en estos resultados, se presenta a continuación un análisis de brechas, el cual constituye un método para identificar y evaluar las diferencias entre el desempeño actual y el desempeño esperado en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la Agencia Logística de las Fuerzas Militares (ALFM). El término "brecha" se refiere al espacio existente entre el estado actual de la entidad, es decir, "donde estamos ahora", y el estado objetivo deseado, o "donde queremos estar".

Este análisis permite identificar áreas específicas donde los controles, procesos o prácticas actuales no cumplen completamente con los requisitos establecidos por el Modelo de Seguridad y Privacidad de la Información (MSPI). Además, proporciona una base para priorizar acciones correctivas y desarrollar estrategias que cierren estas brechas, optimizando la alineación del SGSI con los objetivos estratégicos de la organización y los estándares internacionales.

Figura 1.
Brecha anexa "A" ISO 27001:2013.

Nota. Identificación brecha anexo "A" ISO 27001:2013 Anexo "A" – Instrumento de identificación de la línea base de seguridad, autodiagnóstico Modelo de Seguridad y Privacidad de la Información – MSPI, ejecución vigencia (2024).

5.2. ALINEACIÓN CON EL PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN (PETI).

Continuando con la ejecución de los proyectos descritos en el Plan Estratégico de Tecnologías de la Información (PETI) y tomando como referencia los resultados y avances logrados en periodos anteriores, para la vigencia 2025 se dará continuidad al desarrollo de actividades orientadas al fortalecimiento y mejoramiento del Modelo de Seguridad y Privacidad de la Información (MSPI). Estas acciones se enmarcan dentro del proyecto de Política de Gobierno Digital de la entidad, asegurando una alineación con los lineamientos establecidos a nivel nacional e internacional.

De igual manera, la ejecución de las actividades señaladas en este plan contribuirá al cumplimiento efectivo de las políticas institucionales de Seguridad de la Información, Seguridad Digital y la Política de Gobierno Digital, fortaleciendo los procesos estratégicos de la organización. Esto permitirá no solo garantizar la confidencialidad, integridad y disponibilidad de los activos de información, sino también avanzar en la consolidación de un entorno tecnológico seguro, confiable y alineado con las normativas vigentes.

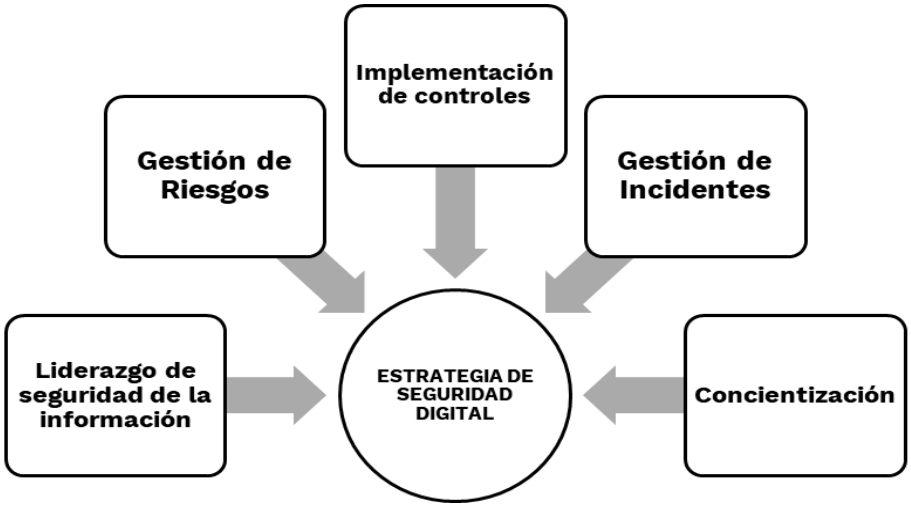
5.3. ESTRATEGIA DE SEGURIDAD DIGITAL.

La Agencia Logística de las Fuerzas Militares (ALFM) implementará una estrategia integral de seguridad digital que integre principios, políticas, procedimientos, guías, manuales, formatos y lineamientos orientados a la gestión efectiva de la seguridad de la información. Esta estrategia tendrá como eje central la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), complementado con la Guía de Gestión de Riesgos de Seguridad de la Información y el Procedimiento de Gestión de Incidentes establecidos por la entidad.

Dicha estrategia buscará garantizar la protección, confidencialidad, integridad y disponibilidad de los activos de información, asegurando el cumplimiento de las normativas nacionales e internacionales aplicables, así como la alineación con las prioridades estratégicas de la entidad.

En este marco, la ALFM define las siguientes cinco (05) estrategias específicas, diseñadas para consolidar un enfoque robusto y proactivo de seguridad digital, y que en conjunto conformarán una estrategia general:

Figura 2.
Estrategia de seguridad digital.



Nota. Especificación estrategia de seguridad digital – Manual de Gobierno Digital (2022).

5.3.1. Descripción de las estrategias especificas (Ejes).

A continuación, se presentan los objetivos de cada una de las estrategias específicas a implementar, estableciendo su alineación con las actividades descritas en el Modelo de Seguridad y Privacidad de la Información (MSPI) y en la Resolución 500 de 2021. Estas estrategias tienen como propósito garantizar el cumplimiento de los lineamientos normativos, fortalecer la seguridad digital de la entidad y asegurar la protección de los activos de información.

Tabla 3.
Descripción estrategias específicas.

ESTRATEGIA / EJE	DESCRIPCIÓN / OBJETIVO
Liderazgo de seguridad de la información.	Asegurar la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) mediante la aprobación de la política general y los lineamientos definidos, con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información. Esta estrategia se fundamenta en el compromiso activo de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la entidad, quienes serán responsables de garantizar el cumplimiento de los roles y responsabilidades establecidos en materia de seguridad de la información. El enfoque central radica en crear una estructura sólida que permita gestionar eficazmente los riesgos asociados a la información, fomentando una cultura organizacional orientada a la seguridad y asegurando que todos los niveles de la entidad contribuyan al fortalecimiento del MSPI.
Gestión de riesgos.	Determinar los riesgos de seguridad de la información mediante un proceso estructurado de planificación y valoración, orientado a prevenir o mitigar los efectos indeseados asociados a dichos riesgos. Esta estrategia se fundamenta en la implementación de controles de seguridad específicos y efectivos, diseñados para el tratamiento adecuado de los riesgos identificados. El enfoque se centra en garantizar que los controles estén alineados con los objetivos estratégicos de la entidad y las normativas aplicables, promoviendo la protección de la confidencialidad, integridad y disponibilidad de los activos de información. Asimismo, este proceso permitirá priorizar acciones correctivas y establecer medidas proactivas para fortalecer la seguridad de la información en todos los niveles de la entidad.
Concientización.	Fortalecer la construcción de una cultura organizacional sólida basada en la seguridad de la información, para que se convierta en un hábito cotidiano en todos los niveles de la entidad. Esto incluye la promoción activa de las políticas, procedimientos, normas, buenas prácticas y demás lineamientos establecidos. Es crucial fomentar la transferencia de conocimiento y la asignación clara de responsabilidades, asegurando que todos los funcionarios estén informados sobre su rol en la seguridad y privacidad de la información. A través de estas acciones, se busca no solo garantizar el

	cumplimiento de las normativas internas, sino también crear una cultura organizacional en la que la protección de la información sea un valor compartido por todos, apoyando la continuidad operativa y la confianza de las partes interesadas.
Implementación de controles.	Planificar e implementar las acciones necesarias para alcanzar los objetivos de seguridad y privacidad de la información es fundamental para mantener la confianza en la ejecución de los procesos de la entidad. Estas acciones se pueden subdividir en dos categorías principales: controles técnicos y controles administrativos. Controles técnicos: Se enfocan en la implementación de herramientas y tecnologías específicas que protejan la infraestructura de la información, tales como firewalls, cifrado de datos, sistemas de detección de intrusos (IDS), y soluciones de autenticación multifactorial. Controles administrativos: Se refieren a políticas, procedimientos, y prácticas de gestión que garantizan la correcta administración de la seguridad de la información. Esto incluye la asignación de responsabilidades claras, capacitación continua del personal, auditorías internas, y el establecimiento de procedimientos para la gestión de incidentes y riesgos. La correcta integración y ejecución de ambos tipos de controles es esencial para proteger los activos de información y asegurar la continuidad operativa dentro de la entidad.
Gestión de incidentes.	Garantizar una gestión eficiente de los incidentes de seguridad de la información mediante un enfoque integral que abarque la integración, el análisis y la comunicación de los eventos e incidentes de seguridad, así como de las debilidades de seguridad detectadas. Este enfoque tiene como objetivo identificar, comprender y resolver estos incidentes de manera efectiva, minimizando su impacto negativo en la entidad. La gestión adecuada de incidentes no solo ayuda a mitigar los riesgos inmediatos, sino que también proporciona información valiosa para fortalecer las defensas a largo plazo, promoviendo un entorno seguro y resiliente.

Nota. Descripción estrategias especificas a implementar de acuerdo a los lineamientos de la resolución 500 de 2021. Producto tipo PESI MinTIC (2022).

5.4. RESPONSABILIDADES.

Tabla 4.
Descripción responsabilidades frente a la implementación del MSPI.

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
Alta Dirección	Conocer el diseño e implementación del Sistema de Gestión de Seguridad de la Información – SGSI de la ALFM. Garantizar el cumplimiento de los objetivos y políticas institucionales a través del cumplimiento del SGSI. Asegurar mediante la revisión por la dirección que el SGSI sea conveniente, adecuado y eficaz para la entidad. Asegurar que se establezcan y mantengan los procesos necesarios para asegurar la confidencialidad, integridad y disponibilidad de los activos de información. Definir, asignar y aprobar los recursos financieros, técnicos, económicos y el personal necesario para el diseño, implementación, evaluación y mejora del SGSI. Establecer la Política de seguridad de la información, para garantizar la divulgación y la comunicación de esta a la ALFM. Garantizar el cumplimiento de la normatividad legal vigente aplicable en materia de Seguridad de la Información. Evaluar mínimo una vez al año la implementación de políticas y lineamientos en materia de seguridad de la información al interior de la ALFM. Conocer los avances, resultados, operación y efectividad de las acciones emprendidas en Seguridad de la Información.
Comité Institucional de Gestión y Desempeño.	Análisis de los resultados obtenidos en el diagnóstico inicial del Modelo de Seguridad y Privacidad de la Información – MSPI.

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
	Conocer y analizar la política de Seguridad establecida en la ALFM. Apoyo en la implementación de los estándares de seguridad necesarios, que garanticen la confidencialidad, integridad y disponibilidad de los activos de información. Participar en la investigación de incidentes de seguridad materializados. Conocer, entender y aplicar las políticas, normas, reglamentos, instrucciones e instructivos definidos en el SGSI. Proponer a la alta dirección la opción de medidas y desarrollo de actividades que procuren y mantengan el aseguramiento de los activos de información, preservando la confidencialidad, integridad y disponibilidad, en lo referente al SGSI. Vigilar el desarrollo de las actividades llevadas a cabo frente a la implementación y mejora del SGSI. Conocer los avances, resultados, operación y efectividad de las acciones emprendidas en Seguridad de la información. Realizar seguimiento a los indicadores del SGSI y el análisis de estos.
Líder Proceso Gestión de TIC.	Orientar y coordinar con los funcionarios requeridos, los procesos de implementación, desarrollo y mantenimiento del SGSI. Proponer acciones correctivas o de mejora a la alta dirección, ante la aparición de problemas potenciales o reales en la implementación y sostenibilidad del SGSI. Representar a la ALFM, en asuntos relacionados con el SGSI, ante organismos externos.

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
	Informar a la alta Dirección sobre el desempeño y las oportunidades de mejora del SGSI (NTC/ISO 27001:2013). Propender la concientización de los requisitos, necesidades y expectativas de las partes interesadas e involucradas en el SGSI en todos los niveles de la ALFM. Trabajar en coordinación con los Directores, Subdirectores, Jefes de Oficina y coordinadores de la ALFM, en el proceso de implementación y sostenibilidad del SGSI, diseñando planes y acciones necesarias para el cumplimiento del propósito.
Profesional Seguridad de la Información.	Evaluar por lo menos una vez al año el desarrollo de las políticas y lineamientos establecidos en el SGSI. Coordinar las actividades definidas para la sensibilización y capacitación a los funcionarios, contratistas y terceros relacionados con la ALFM, en temas de seguridad de la información. Establecer, cumplir y hacer cumplir las políticas definidas en el SGSI. Identificar, evaluar y valorar los riesgos, así como contribuir en el control de estos. Establecer y socializar los planes de seguridad y privacidad de la información establecidos al interior de la ALFM. Diseñar e implementar el SGSI en la ALFM. Diseñar y gestionar la aprobación de los planes de seguridad de la información por parte de la alta dirección, así como ejecutarlo y hacer seguimiento para alcanzar los objetivos del SGSI. Informar a la alta dirección y a los funcionarios, sobre el funcionamiento, avances y los resultados del SGSI.

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
	Promover la participación de los funcionarios de la ALFM, en la implementación del SGSI. Elaborar, actualizar y divulgar normas de seguridad, instructivos, programas, procedimientos, reglamentos, objetivos y metas del SGSI. Participar como invitado en las reuniones del Comité Integral de Gestión y Desempeño, apoyando su gestión. Participar y liderar en la investigación y detección de los Incidentes, reportándolos, documentándolos y generando buenas prácticas al respecto mediante la difusión de boletines de seguridad. Garantizar la gestión del cumplimiento normativo y de las divulgaciones referentes al SGSI. Realizar verificaciones de la implementación y adopción de políticas de seguridad, al interior de la entidad, preservando la confidencialidad, integridad y disponibilidad de los activos de información. Capacitar y motivar a los funcionarios para el cumplimiento de las normas y políticas de seguridad de la información en la ALFM. Solicitar los recursos requeridos para el diseño e implementación del SGSI.
Líderes de Proceso.	Revisar los procedimientos y demás documentos propios de sus procesos frente a la ejecución del SGSI y ajustarlos si es necesario. Asegurar el cumplimiento de las políticas de seguridad establecidas en cada uno de los procesos que lidera y los transversales en lo que le compete. Verificar la identificación, evaluación, tratamiento y seguimiento de los riesgos sobre la seguridad de la información en su proceso, así mismo su pertinencia. Garantizar que todo su personal cumpla con las

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
	políticas, lineamientos y demás documentos generados en el SGSI. Motivar y permitir la asistencia de los funcionarios a cargo, a las sesiones de sensibilización y capacitación en temas relacionados con la seguridad de la información. Conocer los avances, resultados, operación y efectividad de las acciones emprendidas en el SGSI. Reportar oportunamente los incidentes de seguridad de la información a la Oficina Gestión de TIC, incumplimientos de políticas de seguridad y condiciones inseguras al interior de sus procesos, así mismo, motivar al personal a su cargo el reporte oportuno de los mismos. Responsabilizarse por la seguridad de los activos de información de su proceso, apoyándose en cada uno de los custodios (funcionarios) delegados en la protección de estos. Cumplir y hacer cumplir las normas, reglamentos, instrucciones, programas, políticas y planes establecidos en el SGSI, dentro del área a su cargo. Mantener retroalimentación de los procesos bajo su responsabilidad mediante la implementación de acciones correctivas, preventivas y de mejora del SGSI.
Funcionarios – Contratistas.	Participar activamente de las actividades establecidas en cada uno de los procedimientos que hacen parte del SGSI. Dar cumplimiento a las políticas establecidas en el SGSI. Participar de las capacitaciones y actividades relacionadas con el SGSI. Utilizar adecuadamente los activos de información suministrados para el desarrollo de sus labores,

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
	dándole el uso debido. Velar por la conservación de los activos de información de la ALFM, siguiendo las recomendaciones establecidas en los programas de SGSI aplicables a cada proceso. Informar oportunamente a su Jefe inmediato y el profesional de seguridad de la información sobre los riesgos de seguridad informática latentes en su sitio de trabajo. Establecer con el líder del proceso la necesidad de capacitaciones relacionadas con la seguridad de la información de acuerdo con las actividades a realizar. Reportar oportunamente los incidentes de seguridad, incumplimientos de políticas de seguridad y condiciones inseguras al interior de sus procesos. Conocer, entender y aplicar las políticas, normas, reglamentos, instrucciones e instructivos definidos en el SGSI. Participar en las actividades de sensibilización y capacitación sobre temas relacionados con la seguridad de la información. Dar cumplimiento de los objetivos del SGSI. Mantener limpio y ordenado el puesto de trabajo, preservando la confidencialidad de la información bajo su responsabilidad. Cumplir con todos los requisitos, cláusulas y demás parámetros legales y contractuales establecidos por la ALFM para el buen desempeño del SGSI.
Responsabilidades de los Visitantes	Cumplir las normas, reglamentos, instrucciones, programas, políticas y planes establecidos en el SGSI al interior de la ALFM.

Nota. Descripción matriz de roles y responsabilidades sistema de gestión de seguridad de la información – SGSI Código: GTI-DG-02 Versión No. 00. Suite Vision Empresarial ALFM (2022).

6. MATRIZ DE ACTIVIDADES

Tabla 5.
Definición de actividades, establecidas por estrategia.

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO
Liderazgo de seguridad de la información.	Implementación MSPI.	Análisis GAP para identificar el estado actual de la entidad en relación con la adopción del MSPI.	Anexo 1. Modelo de Seguridad y Privacidad de la Información (Feb/2021).	Plazo: Primer Bimestre. Evidencia: Informe del análisis GAP realizado.
		Seguimiento al avance en la implementación del MSPI.	Modelo de Seguridad y Privacidad de la Información (Jul/2016). Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información (Jun/2017). Anexo 1. Modelo de Seguridad y Privacidad de la Información (Feb/2021). Instrumento de Autoevaluación del Modelo de Seguridad y Privacidad de la Información (Nov/2022).	Plazo: Trimestral. Evidencia: Informe de seguimiento implementación MSPI, anexando el instrumento de evaluación del MSPI actualizado.
		Realizar un proceso de análisis y verificación de la ejecución de las actividades definidas en el Plan Estratégico de Seguridad de la Información - PESI. Este análisis estará orientado a identificar ajustes y/o cambios necesarios para garantizar el cumplimiento de la normativa aplicable y los objetivos de la misión institucional.		Plazo: Anual. Evidencia: Informe de Análisis y Verificación del Plan Estratégico de Seguridad de la Información (PESI).
	Análisis para determinar la necesidad de actualizar las políticas de seguridad de la información.	Resultado del análisis que determina si es necesario actualizar o mantener el Manual de Políticas de Seguridad de la Información en su estado actual.	Guía No. 08 – Controles de Seguridad y Privacidad de la Información (Mar/2016). Anexo 1. Modelo de Seguridad y Privacidad de la Información	Plazo: Primer Semestre. Evidencia: Documento que justifica la decisión de no actualizar el Manual de Políticas de Seguridad de la Información o la versión actualizada

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO
			(Feb/2021).	del mismo.
		Resultado del análisis que determina si es necesario actualizar o mantener la Declaración de Aplicabilidad en su estado actual.	Guía elaboración Manual de Políticas de Seguridad de la Información (Nov/2022).	Plazo: Primer Semestre. Evidencia: Documento que justifica la decisión de no actualizar la Declaración de Aplicabilidad o la versión actualizada del mismo.
		Resultado del análisis que determina si es necesario actualizar o mantener la Matriz de Roles y Responsabilidades de Seguridad de la Información en su estado actual.	Anexo 1. Modelo de Seguridad y Privacidad de la Información (Feb/2021). Roles y Responsabilidades MSPI (Oct/2021).	Plazo: Primer Semestre. Evidencia: Documento que justifica la decisión de no actualizar la Matriz de Roles y Responsabilidades del MSPI o la versión actualizada del mismo.
		Resultado del análisis que determina si es necesario actualizar o mantener la Política General de Seguridad de la Información en su estado actual.	Guía No. 2 – Elaboración de la Política general de seguridad y privacidad de la información. Anexo 1. Modelo de Seguridad y Privacidad de la Información (Feb/2021). Guía elaboración Política General de Seguridad de la Información (Nov/2022).	Plazo: Primer Semestre. Evidencia: Documento que justifica la decisión de no actualizar la Política General de Seguridad y Privacidad de la Información o la versión actualizada del mismo.
	Inventario de Activos de Información.	Actualización del inventario de activos de información.	Guía No. 5 – Guía para la Gestión y Clasificación de Activos de Información (Mar/2016). Formato Inventario y Clasificación de Activos de Información (Nov/2022).	Plazo: Primer Cuatrimestre. Evidencia: Guía para la gestión y clasificación de activos de información actualizada.
				Plazo: Primer Cuatrimestre. Evidencia: Acta(s) de

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO
				reunión(es), mediante la cual se designan los responsables de gestionar las Matrices de Activos de Información por Procesos y Regionales.
				Plazo: Semestral. Evidencia: Matriz de activos de información actualizada. (Actividades por Proceso y Regionales).
		Realizar un análisis integral de la actualización de los activos de información para identificar el impacto en los riesgos de TIC, el Plan de Tratamiento de Riesgos (PTR) y los indicadores de gestión, con el fin de determinar la necesidad de ajustes en los controles y parámetros de medición establecidos.		Plazo: Semestral. Evidencia: Documento que registre el análisis realizado, incluyendo la justificación de los ajustes o cambios propuestos (si aplica) en los riesgos de TIC, el PTR y los indicadores de gestión, en función de la actualización de los activos de información.
	Gestión Plan de Continuidad del Negocio ALFM.	Seguimiento gestión plan de continuidad del negocio TIC ALFM.	Anexo 1. Modelo de Seguridad y Privacidad de la Información (Feb/2021). Guía No. 11 – Guía para realizar el Análisis de Impacto de Negocios BIA (May/2015).	Plazo: Primer Trimestre. Evidencia: Documento que justifica la decisión de no actualizar los formatos Evaluación Evento Activación Plan de Continuidad, Diseño y Ejecución de Pruebas de Recuperación y Evaluación Pruebas de Recuperación o las versiones actualizadas del

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO
				mismo.
				Plazo: Primer Trimestre. Evidencia: Plan de Continuidad del Negocio TIC ajustado a la vigencia.
				Plazo: Semestral. Evidencia: Informe de seguimiento al cumplimiento de actividades establecidas, mediante el Plan de Continuidad del negocio TIC.
Gestión de riesgos.	Gestión Plan de Tratamiento de Riesgos de seguridad y privacidad de la información.	Seguimiento al estado avance del Plan.	Guía No. 7 – Guía de gestión de riesgos (Abr/2016). Matriz de Riesgos de Seguridad de la Información (Nov/2022).	Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de actividades establecidas, mediante el Plan de Tratamiento de Riesgos de seguridad y Privacidad de la Información.
Concientización.	Plan de sensibilización anual funcionarios de la ALFM.	Plan de actividades de sensibilización y concientización en temas relacionados a seguridad digital y de la información dirigido a todos los funcionarios de la entidad.	Guía No. 14 – Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información (Mar/2016).	Plazo: Primer Bimestre. Evidencia: Plan de sensibilización y capacitación a los funcionarios de la ALFM.
				Plazo: Semestral. Evidencia: Informes de seguimiento a la ejecución del plan de actividades de sensibilización y concientización.
Implementación de controles.	Gestión controles Administrativos y Técnicos del MSPI.	Incremento progresivo de controles administrativos (A.5, A.6, A.7, A.8, A.15, A.17, A.18).	Guía No. 08 – Controles de Seguridad y Privacidad de la Información (Mar/2016). Modelo de	Plazo: Primer Cuatrimestre. Evidencia: Documento que justifica la decisión de no actualizar los Acuerdos de

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO
			Seguridad y Privacidad de la Información (Jul/2016). Anexo 1. Modelo de Seguridad y Privacidad de la Información (Feb/2021). Instrumento de Autoevaluación del Modelo de Seguridad y Privacidad de la Información (Nov/2022).	Confidencialidad y No Divulgación de funcionarios y/o Contratistas o las versiones actualizadas del mismo.
				Plazo: Primer Cuatrimestre. Evidencia: Documento que defina los lineamientos para la asignación y/o devolución de activos de funcionarios y/o terceros.
		Incremento progresivo de controles técnicos (A.9, A.10, A.11, A.12, A.13, A.14, A.16).		Plazo: Semestral. Evidencia: Informes de seguimiento a la aplicabilidad de la Guía de Control de Acceso Basada en Roles (RBAC).
				Plazo: Primer Cuatrimestre. Evidencia: Documento que soporte la definición de lineamientos para el registro de accesos (logs de acceso a sistemas, servidores, etc).
				Plazo: Semestral. Evidencia: Informes de seguimiento al control de registro de accesos (logs de acceso a sistemas, servidores, etc).
				Plazo: Primer Cuatrimestre. Evidencia: Documento que soporte la definición de lineamientos para la gestión de cambios en los sistemas, servidores, etc.

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO
				Plazo: Semestral. Evidencia: Informes de seguimiento a la aplicabilidad de gestión de cambios en los sistemas, servidores, etc.
				Plazo: Primer Cuatrimestre. Evidencia: Documento que soporte la definición de lineamientos en los acuerdos de nivel de servicio de las mesas de ayuda tecnológicas (GLPI - SOLMAN).
				Plazo: Cuatrimestral. Evidencia: Informes de seguimiento a los registros de trafico de red de los perfiles de navegación medio y alto.
Gestión de incidentes.	Prevención de eventos de seguridad informática.	Procedimientos documentados para la gestión de incidentes.	Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información (Jun/2021). Formato Reporte de Incidentes CSIRT Gobierno – Versión 3 (Nov/2022). Formato Reporte de Eventos No Críticos (Nov/2022).	Plazo: Primer Cuatrimestre. Evidencia: Documento que justifica la decisión de no actualizar el Procedimiento de Seguridad de la Información o la versión actualizada del mismo.
				Plazo: Primer Semestre. Evidencia: Documento que soporte la definición de lineamientos para la gestión de incidentes de seguridad de la información.
		Intercambiar y/o compartir con el CSIRT, COLCERT, CAIVIRUTAL,		Plazo: Cuatrimestral. Evidencia: Soporte de los mensajes de

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO
		(DIJIN) y CCOC para apoyar la gestión de riesgos y la toma de decisiones (priorización, tratamiento y aceptación, respuesta a incidentes), especialmente, para prevenir interna y externamente amenazas cibernéticas.		correos electrónicos generados.
		Informes de seguimiento a los eventos de seguridad presentados (Fortisandbox).		Plazo: Cuatrimestral. Evidencia: Informes de seguimiento eventos de seguridad.

Nota. Definición de actividades a ejecutar establecidas por estrategia para la vigencia 2025. Producto tipo PESI MinTIC "Portafolio de proyectos/actividades" (2022).

7. SEGUIMIENTO

A través de la herramienta Suite visión empresarial, se realizará el cargue y seguimiento a las tareas planeadas y estructuradas como se describe en la matriz de actividades anexa y de acuerdo al análisis realizado por el Profesional Defensa – Seguridad de la Información de la Oficina principal. De igual manera, a través del seguimiento mediante el instrumento de identificación de la línea base de seguridad – Modelo de Seguridad y Privacidad de la Información – MSPI 2025.

8. ANÁLISIS Y MEDICIÓN

El análisis y medición de la ejecución del Plan Estratégico de Seguridad y Privacidad de la Información (PESI) estará cargo de la Jefatura de la Oficina TIC. En atención al Decreto 612 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", en su artículo 1. Adicionar al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, los siguientes artículos "2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción; las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos…"; por lo consiguiente, de acuerdo con mesas de trabajo adelantadas se realizará la articulación del: Plan Estratégico de Seguridad y Privacidad de la Información (PESI) a través de informes trimestrales de avance a su cumplimiento.

ANEXO

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
Análisis GAP para identificar el estado actual de la entidad en relación con la adopción del MSPI.	Informe del análisis GAP realizado en la adopción del MSPI.	01/02/2025	07/03/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Seguimiento al avance en la implementación del MSPI.	Informe de seguimiento implementación MSPI, anexando el instrumento de evaluación del MSPI actualizado.	01/02/2025 01/04/2025 01/07/2025 01/10/2025	07/04/2025 07/07/2025 07/10/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Realizar un proceso de análisis y verificación de la ejecución de las actividades definidas en el Plan Estratégico de Seguridad de la Información - PESI. Este análisis estará orientado a identificar ajustes y/o cambios necesarios para	Informe de Análisis y Verificación del Plan Estratégico de Seguridad de la Información (PESI).	01/01/2026	15/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
garantizar el cumplimiento de la normativa aplicable y los objetivos de la misión institucional.								
Resultado del análisis que determina si es necesario actualizar o mantener el Manual de Políticas de Seguridad de la Información en su estado actual.	Documento que justifica la decisión de no actualizar el Manual de Políticas de Seguridad de la Información o la versión actualizada del mismo.	01/02/2025	07/07/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Resultado del análisis que determina si es necesario actualizar o mantener la Declaración de Aplicabilidad en su estado actual.	Documento que justifica la decisión de no actualizar la Declaración de Aplicabilidad o la versión actualizada del mismo.	01/02/2025	07/07/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Resultado del análisis que determina si es necesario actualizar o	Documento que justifica la decisión de no actualizar la Matriz de Roles y	01/02/2025	07/07/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
mantener la Matriz de Roles y Responsabilidades de Seguridad de la Información en su estado actual.	Responsabilidades del MSPI o la versión actualizada del mismo.							
Resultado del análisis que determina si es necesario actualizar o mantener la Política General de Seguridad de la Información en su estado actual.	Documento que justifica la decisión de no actualizar la Política General de Seguridad y Privacidad de la Información o la versión actualizada del mismo.	01/02/2025	07/07/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Actualización del inventario de activos de información.	Guía para la gestión y clasificación de activos de información actualizada.	01/02/2025	08/05/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
	Acta(s) de reunión(es), mediante la cual se designan los responsables de gestionar las Matrices de Activos de Información por	01/02/2025	08/05/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
	Procesos y Regionales.							
	Matriz de activos de información actualizada. (Actividades por Proceso y Regionales).	01/02/2025 01/07/2025	07/07/2025 07/01/2026	Todos los Procesos.	Todos los Procesos.	Técnicos de Apoyo Seguridad y Defensa. Profesionales Defensa. Procesos y Regionales ALFM.	Profesional Defensa.	Líder Proceso Gestión de TIC.
Realizar un análisis integral de la actualización de los activos de información para identificar el impacto en los riesgos de TIC, el Plan de Tratamiento de Riesgos (PTR) y los indicadores de gestión, con el fin de determinar la necesidad de ajustes en los controles y parámetros de	Documento que registre el análisis realizado, incluyendo la justificación de los ajustes o cambios propuestos (si aplica) en los riesgos de TIC, el PTR y los indicadores de gestión, en función de la actualización de los activos de información.	01/02/2025 01/07/2025	07/07/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
medición establecidos.								
Seguimiento gestión plan de continuidad del negocio TIC ALFM.	Documento que justifica la decisión de no actualizar los formatos Evaluación Evento Activación Plan de Continuidad, Diseño y Ejecución de Pruebas de Recuperación y Evaluación Pruebas de Recuperación o las versiones actualizadas del mismo.	01/02/2025	07/04/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
	Plan de Continuidad del Negocio TIC ajustado a la vigencia.	01/02/2025	07/04/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
	Informe de seguimiento al cumplimiento de actividades establecidas, mediante el Plan de Continuidad	01/02/2025 01/07/2025	07/07/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
	del negocio TIC.							
Seguimiento al estado avance del Plan de Tratamiento de Riesgos de seguridad y privacidad de la información.	Informe de seguimiento al cumplimiento de actividades establecidas, mediante el Plan de Tratamiento de Riesgos de seguridad y Privacidad de la Información.	01/02/2025 01/05/2025 01/09/2025	08/05/2025 05/09/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Plan de actividades de sensibilización y concientización en temas relacionados a seguridad digital y de la información dirigido a todos los funcionarios de la entidad.	Plan de sensibilización y capacitación a los funcionarios de la ALFM.	01/02/2025	07/03/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
	Informes de seguimiento a la ejecución del plan de actividades de sensibilización y concientización.	01/02/2025 01/07/2025	07/07/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Incremento progresivo de controles administrativos (A.5, A.6, A.7, A.8, A.15, A.17, A.18).	Documento que justifica la decisión de no actualizar los Acuerdos de Confidencialidad y No Divulgación de funcionarios y/o	01/02/2025	08/05/2025	Oficina Tecnologías de la Información y las Comunicaciones. Subdirección General de Contratación.	Proceso Gestión de TIC. Proceso Gestión de la Contratación.	Profesionales Defensa – Seguridad de la Información - Subdirección General de Contratación – Grupo	Profesional Defensa – Seguridad de la Información.	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
	Contratistas o las versiones actualizadas del mismo.			Dirección Administrativa y Talento Humano.	Proceso Gestión de Talento Humano.	Administración y Desarrollo del Talento Humano.		
	Documento que defina los lineamientos para la asignación y/o devolución de activos de funcionarios y/o terceros.	01/02/2025	08/05/2025	Dirección Administrativa y Talento Humano.	Proceso Gestión Administrativa.	Profesional Defensa – Grupo Servicios Administrativos.	Profesional Defensa – Seguridad de la Información.	Líder Proceso Gestión de TIC.
Incremento progresivo de controles técnicos (A.9, A.10, A.11, A.12, A.13, A.14, A.16).	Informes de seguimiento a la aplicabilidad de la Guía de Control de Acceso Basada en Roles (RBAC).	01/02/2025 01/07/2025	07/07/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
	Documento que soporte la definición de lineamientos para el registro de accesos (logs de acceso a sistemas, servidores, etc).	01/02/2024	08/05/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Grupo Redes e Infraestructura Tecnológica y Grupo Informática.	Profesional Defensa – Seguridad de la Información.	Líder Proceso Gestión de TIC.
	Informes de seguimiento al control de registro de accesos (logs de	01/02/2025 01/07/2025	07/07/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
	acceso a sistemas, servidores, etc).							
	Documento que soporte la definición de lineamientos para la gestión de cambios en los sistemas, servidores, etc.	01/02/2024	08/05/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Grupo Redes e Infraestructura Tecnológica y Grupo Informática.	N/A	Líder Proceso Gestión de TIC.
	Informes de seguimiento a la aplicabilidad de gestión de cambios en los sistemas, servidores, etc.	01/02/2025 01/07/2025	07/07/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesionales Defensa – Proceso Gestión de TIC.	N/A	Líder Proceso Gestión de TIC.
	Documento que soporte la definición de lineamientos en los acuerdos de nivel de servicio de las mesas de ayuda tecnológicas (GLPI - SOLMAN).	01/02/2024	08/05/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Técnico de Apoyo Seguridad y Defensa – Grupo Informática. Profesional Defensa – Grupo Redes e Infraestructura Tecnológica.	Profesional Defensa – Seguridad de la Información.	Líder Proceso Gestión de TIC.
	Informes de seguimiento a los	01/02/2025 01/05/2025	08/05/2025 05/09/2025	Oficina Tecnologías de la	Proceso Gestión de	Profesional Defensa –	Profesional Defensa –	Líder Proceso Gestión de

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
	registros de trafico de red de los perfiles de navegación medio y alto.	01/09/2025	07/01/2026	Información y las Comunicaciones.	TIC.	Grupo Redes e Infraestructura Tecnológica.	Seguridad de la Información.	TIC.
Procedimientos documentados para la gestión de incidentes.	Documento que justifica la decisión de no actualizar el Procedimiento de Seguridad de la Información o la versión actualizada del mismo.	01/02/2025	08/05/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
	Documento que soporte la definición de lineamientos para la gestión de incidentes de seguridad de la información.	01/02/2025	07/07/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Intercambiar y/o compartir con el CSIRT, COLCERT, CAIVIRUTAL, (DIJIN) y CCOC para apoyar la gestión de riesgos y la toma de decisiones	Soporte de los mensajes de correos electrónicos generados.	01/02/2025 01/05/2025 01/09/2025	08/05/2025 05/09/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
(priorización, tratamiento y aceptación, respuesta a incidentes), especialmente, para prevenir interna y externamente amenazas cibernéticas.								
Seguimiento a los eventos de seguridad presentados.	Informes de seguimiento eventos de seguridad.	01/02/2025 01/05/2025 01/09/2025	08/05/2025 05/09/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.