PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN "PESI" – VIGENCIA 2024.

ELABORÓ	REVISÓ	APROBÓ
NOMBRE: Ing. Deiby Leandro Alvarado Rodríguez.	**NOMBRE:** Ing. Roberto Velásquez Arango	**NOMBRE:** CR. Carlos Augusto Mórales Hernández
CARGO: Profesional Defensa – Seguridad de la información.	**CARGO:** Coordinador Grupo Informática	**CARGO:** Director General de la Agencia Logística de las Fuerzas Militares
FIRMA:	**FIRMA:**	**FIRMA:**

TABLA DE CONTENIDO

1. GENERALIDADES

La Agencia Logística de las Fuerzas Militares (ALFM) ha reconocido que la información es esencial para alcanzar sus objetivos. Por ello, se enfoca en protegerla sin importar cómo se use, procese o guarde. Además, entiende que los sistemas de información respaldan sus procesos, por lo que requiere estrategias eficientes para controlarla.

Para garantizar esta protección, la ALFM ha adoptado metodologías específicas para identificar, valorar y gestionar los riesgos de sus activos de información. El Modelo de Seguridad y Privacidad de la Información (MSPI) establece políticas y procedimientos alineados con la estrategia institucional, con controles monitoreados mediante indicadores y revisiones constantes para identificar mejoras.

En línea con regulaciones gubernamentales, la implementación del MSPI se integra como parte clave de la Política de Gobierno Digital, respaldada por decretos y resoluciones. La entidad sigue lineamientos normativos para mejorar su desempeño y satisfacer las necesidades de sus partes interesadas.

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) refleja los objetivos de la ALFM en el uso efectivo de Tecnologías de la Información y las Comunicaciones (TIC), alineándose completamente con los objetivos estratégicos de la institución.

Los proyectos actuales y futuros se centran en desarrollar, optimizar e implementar sistemas de información efectivos y gestionar la infraestructura tecnológica. Estas iniciativas, basadas en el MSPI y las mejores prácticas, no solo buscan cumplir los objetivos institucionales, sino también generar confianza en el uso de la tecnología.

2. REFERENCIA NORMATIVA

Ley 527 (agosto 18) de 1999 “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.

Ley 594 (julio 14) de 2000 “Por la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.

Ley 599 (julio 14) de 2001 “Código Penal Colombiano”.

Ley 1221 (julio 16) de 2008 “Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones”.

Ley 1266 (diciembre 31) de 2008 “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 (enero 05) de 2009 “Por medio del 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”.

Ley 1581 (octubre 17) de 2012 “Disposiciones Generales para tratamiento de datos personales”.

Ley 1712 (marzo 06) de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública”.

Ley 1978 (julio 25) de 2019 “Por la cual se moderniza el sector de las tecnologías de la información y las comunicaciones – TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones”.

Ley 2052 (agosto 25) de 2020 “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”.

Ley 2294 (mayo 19) de 2023 “Por el cual se expide el plan nacional de desarrollo 2022 – 2026 “Colombia potencia mundial de vida””.

NTC-ISO/IEC 27001 de 2022 “Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información - Requisitos”.

Decreto 2364 (noviembre 22) de 2012 “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 1377 (junio 27) de 2013 “Por el cual se reglamenta parcialmente la ley 1581 de 2012”.

Decreto 2573 (diciembre 12) de 2014 “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 1078 (mayo 26) de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

Decreto 728 (mayo 05) de 2017 “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 (agosto 25) de 2017 “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”.

Decreto 612 (abril 04) 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”.

Decreto 1008 (junio 14) de 2018 “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 620 (mayo 02) de 2020 “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.”

Decreto 45 (enero 15) de 2021 “Por el cual se derogan el decreto 704 de 2018 y el artículo 1.1.2.3. del decreto número 1078 de 2015, único reglamentario del sector de tecnologías de la información y las comunicaciones”.

Decreto 377 (abril 09) de 2021 “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 (enero 24) de 2022 “Por el cual se adiciona el título 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”.

Decreto 338 (marzo 08) de 2022 “Por el cual se adiciona el título 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”.

Decreto 767 (mayo 16) de 2022 “Por la 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 1227 (junio 18) de 2022 “Por el cual se modifican los artículos 2.2.1.5.3, 2.2.1.5.5, 2.2.1.5.8 y 2.2.1.5.9 y se adicionan los artículos 2.2.1.5.15 al 2.2.1.5.25 al Decreto 1072 de 2015, único reglamentario del sector trabajo, relacionados con el teletrabajo.”

Decreto 1263 (julio 22) de 2022 “Por el cual se adiciona el titulo 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.”

CONPES 3701 (julio 14) de 2011 “Lineamientos de política para ciberseguridad y ciberdefensa”.

CONPES 3854 (abril 11) de 2016 “Política Nacional de Seguridad Digital”.

CONPES 3920 (abril 17) de 2018 “Política nacional de explotación de datos (BIG DATA)”.

CONPES 3995 (julio 01) de 2020 “Nacional de confianza y seguridad Digital”.

Resolución 1519 (agosto 24) de 2020 “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”.

Resolución 413 (marzo 01) de 2021 “Por la cual define el uso de las tecnologías en la nube para el sector defensa y se dictan otras disposiciones”.

Resolución 500 (marzo 10) de 2021 “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.”

Resolución 0463 (febrero 09) de 2022 “Por el cual se define el uso de Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones”.

Resolución 000460 (febrero 15) de 2022 “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”.

Resolución 000746 (marzo 11) de 2022 “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”.

Resolución 7870 (diciembre 26) de 2022 “Por la cual se emite y adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa, y se dictan otras disposiciones”.

Manual integrado de gestión (septiembre 27) de 2019 “Manual integrado de gestión, código: GI-MA-02, versión No. 21”.

Directiva Permanente Ministerio Defensa No. 03 (enero 23) de 2019 “Lineamientos para la definición de la Política de Tratamiento de Datos Personales en el Ministerio de Defensa Nacional”.

Directiva Permanente Ministerio Defensa No. 913 (abril 19) de 2013 “Guías y procedimientos en tecnología de información y comunicaciones para el Sector Defensa”.

Directiva Permanente Ministerio de Defensa No. 018 (junio 19) de 2014 “Políticas de seguridad de la información para el Sector Defensa”.

Directiva Presidencial No. 02 (abril 02) de 2019 “Simplificación de la interacción digital entre los ciudadanos y el estado”.

Directiva Presidencial No. 03 (marzo 15) de 2021 “Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos”.

Directiva Presidencial No. 02 (febrero 24) de 2022 “Por medio del cual se efectúa reiteración de la política pública en materia de seguridad digital”.

3. OBJETIVO DEL PLAN

Establecer estrategias de seguridad y privacidad de la información alineadas con el Modelo de Seguridad de la Información (MSPI), con el propósito de reforzar la integridad, confidencialidad y disponibilidad de los activos de información, generando un entorno digital seguro que promueva la confianza en la gestión de datos.

3.1. OBJETIVOS ESPECÍFICOS

Definir y establecer la estrategia de seguridad digital en la ALFM.

Garantizar la protección de la información en la ALFM para mitigar incidentes, intrusiones no autorizadas, filtraciones de datos y ataques cibernéticos.

Mejorar de forma continua la estrategia de seguridad de la información, a través de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

Garantizar la disponibilidad y funcionalidad de los servicios tecnológicos, minimizando interrupciones y maximizando la eficiencia operativa.

Fortalecer y garantizar la seguridad y privacidad de la información en los procesos y servicios de TI con el fin de preservar la confidencialidad, integridad y disponibilidad.

4. ALCANCE

El PESI, tiene como finalidad el diagnóstico, análisis, definición y planeación del manejo de la seguridad de la información de los procesos que se ejecutan en la ALFM y será actualizado anualmente; estos apoyarán el cumplimiento de los procesos y objetivos propuestos por las diferentes dependencias de la ALFM y está articulado de manera global en relación con la seguridad de la información.

5. CUERPO DEL MANUAL

5.1. ESTADO ACTUAL DE LA ENTIDAD FRENTE AL SGSI

El Modelo de Seguridad y Privacidad de la Información – MSPI, define los lineamientos para la implementación de la estrategia de seguridad digital definidos por MinTIC, el cual contempla su operación basada en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (05) fases las cuales permiten gestionar y mantener adecuadamente la seguridad y privacidad de los activos de información. Por ello se deben abordar las siguientes fases:

Diagnostico:
Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la fase cuatro de mejora continua.

Planificación:
Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo esta la más importante del ciclo.

Operación:
Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

Evaluación de desempeño:
Determinar el sistema y forma de evaluación de la adopción del modelo.

Mejoramiento continuo:
Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

En la ALFM, estas fases se han trabajado durante dos (03) vigencias, lo que ha permitido implementar gradualmente el Sistema de Gestión de Seguridad de la Información – SGSI, conforme a la normatividad y las necesidades de la entidad, a continuación, se presentan los resultados del autodiagnóstico realizado en la vigencia 2023.

Como se puede observar en la siguiente evaluación del avance del ciclo de funcionamiento del modelo de operación (PHVA) para el SGSI, la entidad ha cumplido en un 67% el modelo de operación y en adelante se gestionará el 33% pendiente y se seguirá con las fases de Efectivo y Gestionado.

Sin embargo, debido a las constantes actualizaciones frente a la normatividad en materia, como entidad estamos atentos a los nuevos lineamientos que emita el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC), respecto a la actualización de la norma ISO/IEC 27001:2022 y la estructuración de su anexo "A" – Referencia de controles de la seguridad de la información.

Tabla 1.

Avance ciclo de funcionamiento del modelo de operación (PHVA)

AVANCE PHVA		
COMPONENTE	**% DE AVANCE ACTUAL ENTIDAD**	**% AVANCE ESPERADO**
Planificación	34%	40%
Implementación	16%	20%
Evaluación de desempeño	17%	20%
Mejora continúa	18%	20%
TOTAL	**85%**	**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 (2023).
De igual manera, se llevó a cabo una reevaluación de efectividad de los controles de la norma ISO/IEC 27001:2013, de la cual se tiene la siguiente información para la vigencia 2023.

Tabla 2.

Evaluación de efectividad de controles – ISO 27001:2013 Anexo "A".

DOMINIO		**CALIFICACIÓN ACTUAL**	**CALIFICACIÓN OBJETIVO**	**EFECTIVIDAD DE CONTROL**
A.5	Políticas de Seguridad de la Información.	100	100	OPTIMIZADO
A.6	Organización de la Seguridad de la Información.	68	100	GESTIONADO
A.7	Seguridad de los Recursos Humanos.	78	100	GESTIONADO
A.8	Gestión de Activos.	64	100	GESTIONADO
A.9	Control de Acceso.	78	100	GESTIONADO
A.10	Criptografía.	40	100	REPETIBLE
A.11	Seguridad Física y del Entorno.	65	100	GESTIONADO
A.12	Seguridad de las Operaciones.	69	100	GESTIONADO
A.13	Seguridad de las Comunicaciones.	73	100	GESTIONADO
A.14	Adquisición, Desarrollo y Mantenimiento de Sistemas.	59	100	EFECTIVO
A.15	Relaciones con los proveedores.	60	100	EFECTIVO
A.16	Gestión de Incidentes de Seguridad de la Información.	71	100	GESTIONADO
A.17	Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio.	50	100	EFECTIVO
A.18	Cumplimiento.	66.5	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		**67**	**100**	**GESTIONADO**

Nota: Avance evaluación de efectividad de controles 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 (2023).

Con base en estos resultados, a continuación, se presenta un análisis de brechas, que es un método para evaluar las diferencias entre el desempeño real y el desempeño esperado en la implementación del SGSI en la ALFM; el termino "brecha" se refiere al espacio entre "donde estamos ahora" (el estado actual) y donde "queremos estar" (el estado objetivo).

Figura 1.

Brecha anexo "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 (2023).

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 teniendo en cuenta los resultados y avances obtenidos anteriormente, para la vigencia 2024, se dará continuidad al desarrollo de actividades de fortalecimiento y mejoramiento al Sistema de Gestión de Seguridad de la Información -SGSI dentro del proyecto de Política de Gobierno Digital de la entidad; de igual forma con la ejecución de actividades aquí señaladas también se dará cumplimiento a la implementación y gestión de las políticas institucionales de Seguridad de la Información, Seguridad Digital y la Política de Gobierno Digital.

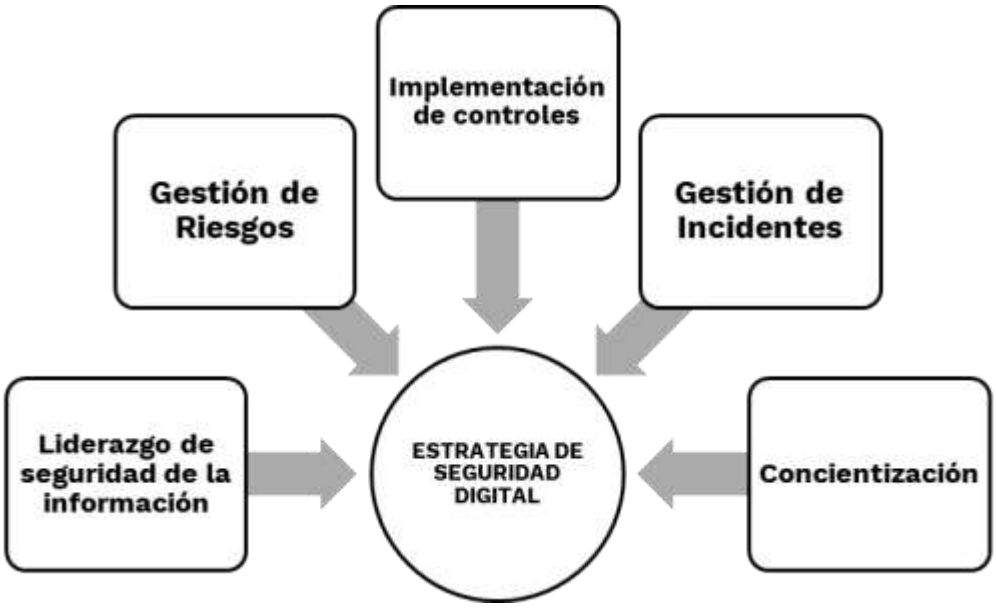
5.2. ESTRATEGIA DE SEGURIDAD DIGITAL.

La ALFM establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, así como la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes establecido por la entidad.

Por tal motivo, la ALFM define las siguientes cinco (05) estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

Figura 2.

Estrategia de seguridad digital.



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

5.2.1. Descripción de las estrategias especificas (Ejes).

A continuación, se describe el objetivo de cada una de las estrategias especificas a implementar, alineando las actividades a los descrito dentro del MSPI y la resolución 500 de 2021:

Tabla 3.

Descripción estrategia especifica.

ESTRATEGIA / EJE	DESCRIPCIÓN / OBJETIVO
Liderazgo de seguridad de la información.	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y

ESTRATEGIA / EJE	DESCRIPCIÓN / OBJETIVO
	disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos.	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados teniendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de riesgos.
Concientización.	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que se convierto en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsables de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles.	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles técnicos y administrativos.
Gestión de incidentes.	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la entidad.

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

5.3. RESPONSABLES

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.

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
	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. 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.
Jefe Oficina 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

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
	implementación y sostenibilidad del SGSI. Representar a la ALFM, en asuntos relacionados con el SGSI, ante organismos externos. 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. 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.

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
	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 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.

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
	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, 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	Seguimiento al estado de avance de implementación del MSPI	Anexo 1. Modelo de Seguridad y Privacidad de la Información. Instrumento evaluación MSPI. Modelo de Seguridad y Privacidad de la Información. Instructivo No. 1 – Diligenciamiento de la Herramienta de diagnóstico de Seguridad y Privacidad de la Información.	Plazo: Trimestral. Evidencia: Informe de seguimiento implementación MSPI, anexando el instrumento de evaluación del MSPI actualizado.
	Inventario de Activos de Información.	Actualización del inventario de activos de información.	Guía No. 5 – Gestión Clasificación de Activos. Inventario y clasificación de Activos de información e Infraestructura critica Cibernética Nacional.	Plazo: Primer Trimestre. Evidencia: Guía para la gestión y clasificación de activos de información actualizada. Plazo: Semestral. Evidencia: Matriz de activos de información actualizada.
	Gestión Plan de Continuidad del Negocio ALFM.	Seguimiento gestión plan de continuidad del negocio TIC ALFM.	Guía No. 10 – Guía para la preparación de las TIC para la continuidad del negocio. Guía No. 11 - Guía	Plazo: Primer Trimestre. Evidencia: Documentos ajustados. (En caso de

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO
			para realizar el Análisis de Impacto de Negocios BIA. Plan de Continuidad del Negocio ALFM	requerirse). Plazo: Semestral. Evidencia: Informe de seguimiento al cumplimiento de actividades establecidas, mediante el Plan de Continuidad del negocio TIC ALFM
Gestión de riesgos.	Gestión Plan de Tratamiento de Riesgos de seguridad y privacidad de la información.	Seguimiento al estado avance del Plan.	Guía No. 07 – Guía de gestión de riesgos.	Plazo: Cuatrimestral. Evidencia: Informe de seguimiento.
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. Convocatorias vigentes lideradas por MinTIC, Gobierno Digital, entidades de seguridad nacional.	Plazo: Primer Bimestre. Evidencia: Plan de sensibilización y capacitación a los funcionarios de la ALFM. Plazo: Cuatrimestral. Evidencia: Informes de seguimiento a la ejecución del plan de actividades de sensibilización y concientización.
Implementación de controles.	Gestión clausulas controles organizacionales, controles de las personas, controles físicos y controles tecnológicos.	Política de Seguridad de la información “General” aprobada por la Alta Dirección. Revisión y actualización manual de políticas de seguridad de la información de acuerdo con la	Guía No. 2 - Elaboración de la política general de seguridad y privacidad de la información. Guía No. 8 - Controles de Seguridad y Privacidad de la Información.	Plazo: Primer Semestre. Evidencia: Documentos ajustados. (En caso de requerirse). Plazo: Primer Semestre. Evidencia: Manual de políticas de seguridad de la información

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO
		actualización de la norma NTC/ISO/IEC 27001:2022.		actualizado.
		Revisión matriz de roles y responsabilidades del SGSI.	Guía No. 4 – Roles y Responsabilidades. Guía No. 5 – Guía para la Gestión y Clasificación de Activos de Información. Guía No. 8 - Controles de Seguridad de la Información.	Plazo: Primer Semestre. Evidencia: Matriz de Roles y responsabilidades ajustada. (En caso de requerirse).
		Revisión acuerdos de confidencialidad y no divulgación a funcionarios y contratistas.	Ley 1581 del 17 de octubre de 2022.	Plazo: Primer Trimestre. Evidencia: Acuerdos de confidencialidad y no divulgación ajustados. (En caso de requerirse).
		Actualización política de tratamiento de datos personales.		Plazo: Primer Trimestre. Evidencia: Política tratamiento de datos personales actualizada.
		Revisión y seguimiento al uso de navegación web, de acuerdo con los perfiles asignados a los funcionarios.	Guía No. 8 - Controles de Seguridad de la Información.	Plazo: Cuatrimestral. Evidencia: Informes de revisión y seguimiento al uso de red (Perfiles de navegación medio y alto).
		Reporte de novedades de personal (retiros, incapacidades, licencias,		Plazo: Trimestral. Evidencia: Soportes del reporte previo

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO
		vacaciones, entre otros).		mediante correo electrónico de las novedades de personal emitidos a la Oficina TIC.
		Revisión periódica del funcionamiento del antivirus adquirido por la entidad.		Actividad que se encuentra integrada al Plan de tratamiento de Riesgos de Seguridad de la Información – PTR, con un plazo de cumplimiento cuatrimestral.
Gestión de incidentes.	Prevención de eventos de seguridad informática.	Intercambiar y/o compartir con el CSIRT, COLCERT, CAIVIRUTAL, (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.	Guía No. 3 - Procedimiento de Seguridad de la Información. Guía No. 8 - Controles de Seguridad de la Información.	Plazo: Cuatrimestral. Evidencia: Mensajes de 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 2024. Producto tipo PESI MinTIC “Portafolio de proyectos/actividades” (2022).

7. SEGUIMIENTO

Articulación con el Plan de Acción Institucional 2024.

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…”. De acuerdo con mesas de trabajo adelantadas se realizará la articulación del: Plan Estratégico de Seguridad y Privacidad de la información - PESI.

Soporte de las actividades publicadas en la plataforma SUITE VISION EMPRESARIAL.

8. ANÁLISIS Y MEDICIÓN

Seguimiento mediante el instrumento de identificación de la línea base de seguridad - Modelo de Seguridad y Privacidad de la Información – MSPI 2024.

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
Seguimiento al estado de avance de implementación del MSPI.	Informe de seguimiento implementación MSPI, anexando el instrumento de evaluación del MSPI actualizado.	01/01/2024 01/04/2024 01/07/2024 01/10/2024	05/04/2024 08/07/2024 04/10/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Actualización del inventario de activos de información.	Guía para la gestión y clasificación de activos de información actualizada.	01/01/2024	05/04/2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
	Matriz de activos de información actualizada.	01/01/2024 01/07/2024	08/07/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Profesional Defensa. Técnicos Regionales.	N/A Profesional Defensa.	Jefe Oficina TIC. Jefe Oficina TIC.
Seguimiento gestión plan de continuidad del negocio TIC ALFM.	Documentos ajustados. (En caso de requerirse).	01/01/2024	05/04/2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
	Informe de seguimiento al cumplimiento de actividades establecidas, mediante el Plan de Continuidad del negocio TIC	01/01/2024 01/07/2024	08/07/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.

	ALFM.							
Seguimiento al estado avance del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Informe de seguimiento ejecución del Plan.	01/01/2024 01/05/2024 01/09/2024	08/05/2024 06/09/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina 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.	01/01/2024	07/03/2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
	Informes de seguimiento a la ejecución del plan de actividades de sensibilización y concientización.	01/01/2024 01/05/2024 01/09/2024	08/05/2024 06/09/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Política de Seguridad de la información “General” aprobada por la Alta Dirección.	Documentos ajustados. (En caso de requerirse).	01/01/2024	08/07/2024	Oficina TIC	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Revisión y actualización manual de políticas de seguridad de la información de acuerdo con la actualización de la norma NTC/ISO/IEC	Manual de políticas de seguridad de la información actualizado.	01/01/2024	08/07/2024	Oficina TIC	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.

27001:2022.								
Revisión matriz de roles y responsabilidades del SGSI.	Matriz de Roles y responsabilidades ajustada. (En caso de requerirse).	01/01/2024	08/07/2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Revisión acuerdos de confidencialidad y no divulgación a funcionarios y contratistas.	Acuerdos de confidencialidad y no divulgación ajustados. (En caso de requerirse).	01/01/2024	05/04/2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Actualización política de tratamiento de datos personales.	Política tratamiento de datos personales actualizada.	01/01/2024	05/04/2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Revisión y seguimiento al uso de navegación web, de acuerdo con los perfiles asignados a los funcionarios.	Informes de revisión y seguimiento al uso de red (Perfiles de navegación medio y alto).	01/01/2024 01/05/2024 01/09/2024	08/05/2024 06/09/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	Profesional Defensa.	Jefe Oficina TIC.
Reporte de novedades de personal (retiros, incapacidades, licencias, vacaciones, entre otros).	Soportes del reporte previo mediante correo electrónico de las novedades de personal emitidos a la Oficina TIC.	01/01/2024 01/04/2024 01/07/2024 01/10/2024	05/04/2024 08/07/2024 07/10/2024 09/01/2025	Dirección Administrativa y de Talento Humano.	Gestión de Talento Humano.	Profesional Defensa.	Profesional Defensa.	Jefe Oficina TIC.
Intercambiar y/o compartir con el CSIRT, COLCERT, CAIVIRUTAL,	Soportes mensajes de correos electrónicos generados.	01/01/2024 01/05/2024 01/09/2024	08/05/2024 06/09/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.

(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.								
Informes de seguimiento a los eventos de seguridad presentados (Fortisandbox).	Informes de seguimiento eventos de seguridad.	01/01/2024 01/05/2024 01/09/2024	08/05/2024 06/09/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.