POLÍTICA GENERAL SEGURIDAD DE LA INFORMACIÓN – AGENCIA LOGÍSTICA DE LAS FUERZAS MILITARES

ELABORÓ	REVISÓ	APROBÓ
NOMBRE: Ing. Deiby Leandro Alvarado Rodríguez.	**NOMBRE:** Ing. Ricardo Valenzuela Díaz. Abo. Martha Eugenia Cortes Baquero. Adm. Jaime Rafel Morón Barros.	**NOMBRE:** Abo. Martha Eugenia Cortes Baquero.
CARGO: Profesional Defensa – Seguridad de la Información.	**CARGO:** Jefe Oficina Tecnologías de la Información y las Comunicaciones. Jefe Oficina Asesora Jurídica. Jefe Oficina Asesora de Planeación e Innovación Institucional.	**CARGO:** Jefe de la Oficina Asesora Jurídica Encargada de las funciones del Despacho de la Dirección General de la Agencia Logística de las Fuerzas Militares.
FIRMA:	**FIRMA:**	**FIRMA:**

TABLA DE CONTENIDO

1. OBJETIVO

Establecer la Política General de Seguridad de la Información de la Agencia Logística de las Fuerzas Militares como el marco institucional para orientar la gestión de la seguridad de la información, mediante la definición de principios, lineamientos y responsabilidades que permitan proteger los activos de información y preservar su confidencialidad, integridad, disponibilidad y, cuando aplique, su autenticidad y trazabilidad, a través de un enfoque basado en la gestión de riesgos, el fortalecimiento de la cultura de seguridad, el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables, el seguimiento, la evaluación y la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), en concordancia con los requisitos de la NTC-ISO/IEC 27001:2022, los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), las políticas de Gobierno Digital y Seguridad Digital, la normativa vigente sobre protección de datos personales y las necesidades y expectativas de las partes interesadas.

2. DEFINICIONES

Para efectos de la presente Política General de Seguridad de la Información, se adoptan las siguientes definiciones con el fin de facilitar la comprensión, interpretación y aplicación de los términos utilizados en este documento.

Activo:	Cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, información, personas, etc.) que tenga valor para la organización.
Activo Crítico:	Son aquellos elementos o componentes que hacen parte de la infraestructura critica.
Activo de Información:	Conocimiento o información que tiene valor para la organización.
Alta Dirección:	Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad. Es la máxima autoridad en el sistema.
Amenaza:	Causa potencial de un incidente no deseado que puede resultar en perjuicio de un sistema o la organización.
Autenticación:	Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
Autenticidad:	Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
Ciberseguridad:	Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.
Confidencialidad:	Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.

Controles:	Medida que permite reducir o mitigar un riesgo.
Custodio:	Individuo, cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de cumplir y velar por el cumplimiento de los controles que el responsable del activo de información haya definido, con base en los controles de seguridad disponibles en la entidad.
Dato personal:	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
Disponibilidad:	Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
Incidente de seguridad de la información:	Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Integridad:	Propiedad de la información que busca preservar su exactitud y completitud.
Modelo Integrado de Planeación y Gestión:	Es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, según dispone el Decreto 1083 de 2015.
NTC-ISO/IEC 27001:	Estándar internacional que establece los requisitos para gestionar la seguridad de la información de una organización. Se aplica a cualquier tipo de organización, independientemente de su tamaño o sector.
Privacidad:	El derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades públicas, la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
Sistema de Gestión de Seguridad de la Información:	Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
Riesgo de seguridad de la información:	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias

3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA AGENCIA LOGÍSTICA DE LAS FUERZAS MILITARES

La Política General de Seguridad de la Información constituye el instrumento mediante el cual la Agencia Logística de las Fuerzas Militares establece los principios, lineamientos y compromisos institucionales para proteger la confidencialidad, integridad, disponibilidad y demás atributos de seguridad de los activos de información que soportan el cumplimiento de su misión.

La Política proporciona el marco de referencia para la implementación, operación, seguimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), orientando la gestión de los riesgos de seguridad de la información, la definición de objetivos, la implementación de controles y el cumplimiento de los requisitos legales, regulatorios, contractuales e institucionales aplicables.

La Alta Dirección aprueba la Política General de Seguridad de la Información y garantiza que esta sea apropiada al contexto de la Agencia Logística de las Fuerzas Militares (ALFM), a su direccionamiento estratégico y a las necesidades y expectativas de las partes interesadas. Asimismo, asegura su alineación con los requisitos aplicables de la Norma ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Gobierno Digital, los lineamientos establecidos para el Sector Defensa y demás disposiciones legales, reglamentarias y normativas aplicables en materia de seguridad de la información, ciberseguridad y protección de la información.

3.1. OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Con el propósito de fortalecer la gestión de la seguridad de la información y contribuir a la protección de los activos de información de la Agencia Logística de las Fuerzas Militares (ALFM), se establecen los siguientes objetivos del Sistema de Gestión de Seguridad de la Información (SGSI), los cuales orientan su planificación, implementación, operación, seguimiento y mejora continua. Estos objetivos se encuentran articulados con el direccionamiento estratégico institucional, la presente Política General de Seguridad de la Información, las necesidades y expectativas de las partes interesadas, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los requisitos aplicables de la Norma ISO/IEC 27001:2022.

3.1.1. Objetivo 1

Proteger los activos de información de la ALFM mediante la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información, garantizando la confidencialidad, integridad y disponibilidad de la información institucional.

3.1.2. Objetivo 2

Gestionar los riesgos de seguridad de la información mediante la identificación, análisis, tratamiento y seguimiento continuo de los riesgos que puedan afectar los procesos institucionales.

3.1.3. Objetivo 3

Fortalecer la cultura institucional de seguridad de la información mediante programas permanentes de sensibilización, capacitación y apropiación de buenas prácticas.

3.1.4. Objetivo 4

Garantizar el cumplimiento de los requisitos legales, regulatorios, contractuales e institucionales aplicables a la seguridad de la información y la privacidad de los datos.

3.1.5. Objetivo 5

Promover la mejora continua del Sistema de Gestión de Seguridad de la Información mediante el seguimiento a indicadores, auditorías, gestión de incidentes, revisión por la Dirección y acciones de mejora.

4. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de la Agencia Logística de las Fuerzas Militares, consciente de la importancia estratégica de la información para el cumplimiento de la misión institucional y la prestación de los servicios a las Fuerzas Militares, demás entidades del Estado y grupos de valor, manifiesta su compromiso con la protección de los activos de información y con el fortalecimiento permanente de la seguridad de la información, la ciberseguridad y la privacidad, mediante el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

En desarrollo de este compromiso, la Alta Dirección garantizará el liderazgo necesario para integrar la seguridad de la información dentro de la planeación estratégica institucional y de los procesos de la Entidad, promoviendo una cultura organizacional basada en la protección de la información, la gestión de riesgos, el cumplimiento de los requisitos legales, regulatorios y contractuales, así como de los lineamientos establecidos por el Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Gobierno Digital y la Norma ISO/IEC 27001:2022.

Así mismo, la Alta Dirección se compromete a:

Aprobar, divulgar y promover el cumplimiento de la presente Política General de Seguridad de la Información y de los demás documentos que conforman el SGSI.

Definir y realizar seguimiento a los objetivos del Sistema de Gestión de Seguridad de la Información, verificando periódicamente su cumplimiento y desempeño.

Asignar y gestionar los recursos humanos, financieros, tecnológicos y de infraestructura necesarios para la implementación, operación, mantenimiento y mejora continua del SGSI.

Promover la identificación, evaluación, tratamiento y seguimiento de los riesgos de seguridad de la información como parte de la gestión institucional.

Fortalecer las competencias y la cultura de seguridad de la información mediante programas permanentes de sensibilización, capacitación y apropiación dirigidos a servidores públicos, contratistas y terceros.

Incorporar la seguridad de la información como un componente transversal en la toma de decisiones estratégicas y en el desarrollo de los proyectos institucionales.

Realizar el seguimiento al desempeño del SGSI mediante la revisión periódica de sus resultados, indicadores, auditorías, incidentes, riesgos y acciones de mejora, en el marco del Comité Institucional de Gestión y Desempeño.

Promover la mejora continua del SGSI, garantizando que este evolucione de acuerdo con los cambios del contexto institucional, tecnológico, normativo y de amenazas que puedan afectar los activos de información de la Entidad.

La Alta Dirección ejercerá este compromiso conforme a las responsabilidades establecidas en la normatividad vigente, incluyendo la Resolución No. 500 de 2021, actualizada por la Resolución No. 2277 de 2025, y las demás disposiciones aplicables en materia de Gobierno Digital, seguridad de la información y gestión institucional.

5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información (SGSI) aplica a la totalidad de la Agencia Logística de las Fuerzas Militares (ALFM), incluyendo la Oficina Principal y todas sus Regionales, así como a los procesos estratégicos, misionales, de apoyo y de evaluación que conforman el Sistema Integrado de Gestión.

El alcance comprende la infraestructura tecnológica institucional, incluyendo centros de procesamiento de datos, servidores, redes de comunicaciones, estaciones de trabajo,

dispositivos móviles, plataformas en la nube, sistemas de información, servicios tecnológicos y demás recursos que soportan la operación de la Entidad.

Igualmente, abarca todos los activos de información administrados por la ALFM, independientemente de su formato físico o digital, así como la información clasificada como pública, pública clasificada y pública reservada, de conformidad con la normativa vigente.

El SGSI aplica a todos los servidores públicos, contratistas, proveedores, terceros y usuarios autorizados que, en ejercicio de sus funciones o actividades, administren, procesen, almacenen, transmitan o tengan acceso a la información institucional o a los recursos tecnológicos de la entidad.

Asimismo, el alcance comprende los procesos relacionados con la gestión de riesgos de seguridad de la información, la gestión de activos de información, la gestión de incidentes de seguridad de la información, la continuidad del negocio, la ciberseguridad, la protección de datos personales, el cumplimiento normativo, el monitoreo, la auditoría y la mejora continua del SGSI, conforme a los lineamientos de la ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Gobierno Digital y las demás disposiciones aplicables.

6. APLICABILIDAD

La presente Política General de Seguridad de la Información, así como los lineamientos, manuales, procedimientos, estándares, instructivos y demás documentos que conforman el Sistema de Gestión de Seguridad de la Información (SGSI), son de obligatorio cumplimiento para todos los servidores públicos, contratistas, proveedores, terceros y demás personas naturales o jurídicas que, en desarrollo de sus funciones, obligaciones contractuales o relaciones con la Agencia Logística de las Fuerzas Militares (ALFM), accedan, administren, procesen, almacenen, transmitan, consulten, intercambien o custodien información institucional o hagan uso de los activos de información y de los recursos tecnológicos de la Entidad.

Igualmente, la presente política será aplicable a las entidades, organismos de control, aliados estratégicos y demás organizaciones externas que, en el marco de las disposiciones legales, reglamentarias o contractuales, tengan acceso autorizado a la información o a los activos de información de la Agencia, quienes deberán cumplir los controles y requisitos de seguridad establecidos por la Entidad, de conformidad con la normatividad vigente y los acuerdos que regulen dicho acceso.

El incumplimiento de las disposiciones establecidas en la presente Política General de Seguridad de la Información y en los demás documentos que conforman el SGSI dará lugar a la aplicación de las medidas administrativas, disciplinarias, contractuales, civiles, penales o de cualquier otra naturaleza que correspondan, de conformidad con la legislación vigente, la normativa interna de la ALFM y las obligaciones derivadas de la relación jurídica aplicable.

La aplicación de esta política se realizará en armonía con los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Gobierno Digital, la Norma ISO/IEC 27001:2022 y las demás disposiciones legales y reglamentarias que regulan la seguridad de la información, la ciberseguridad, la protección de datos personales y la gestión de la información en las entidades públicas.

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

La implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) requieren la participación coordinada de todas las dependencias, servidores públicos, contratistas, proveedores y terceros que, en desarrollo de sus funciones u obligaciones contractuales, administren, procesen, almacenen, transmitan o tengan acceso a los activos de información de la Agencia Logística de las Fuerzas Militares.

La seguridad de la información constituye una responsabilidad compartida y transversal a todos los niveles de la Entidad. En consecuencia, cada actor deberá cumplir las funciones y responsabilidades que le correspondan conforme a su rol, garantizando la aplicación de la Política General de Seguridad de la Información, los lineamientos del SGSI y los controles establecidos para proteger la confidencialidad, integridad, disponibilidad y demás atributos de seguridad de la información institucional.

Las responsabilidades descritas en este capítulo complementan las funciones establecidas en la normatividad vigente, el Manual Específico de Funciones y Competencias Laborales, los actos administrativos internos y los documentos que conforman el Sistema Integrado de Gestión, sin sustituirlas ni modificarlas.

7.1. ALTA DIRECCIÓN

La Alta Dirección es responsable de ejercer el liderazgo y direccionamiento estratégico del Sistema de Gestión de Seguridad de la Información, asegurando su integración con la planeación institucional y con los demás sistemas de gestión de la Entidad.

En desarrollo de este compromiso, le corresponde:

7.1.1. Aprobar la Política de Seguridad de la Información y las modificaciones que se requieran, de acuerdo con las necesidades institucionales y los requisitos aplicables.

7.1.2. Aprobar los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI), en concordancia con los objetivos y lineamientos estratégicos de la entidad.

7.1.3. Asegurar la integración del SGSI con la estrategia institucional y con el Sistema Integrado de Gestión, promoviendo su articulación con los demás sistemas y procesos de la entidad.

7.1.4. Promover una cultura institucional orientada a la protección de la información y al cumplimiento de los principios y lineamientos de seguridad de la información.
7.1.5. Asignar y disponer los recursos humanos, tecnológicos, financieros y técnicos necesarios para la implementación, operación, mantenimiento y mejora continua del SGSI.
7.1.6. Analizar los resultados de la Revisión por la Dirección y adoptar las decisiones y acciones estratégicas necesarias para fortalecer el desempeño y eficacia del SGSI.
7.1.7. Promover la mejora continua del SGSI, mediante la toma de decisiones y el establecimiento de acciones orientadas a fortalecer su desempeño y eficacia.
7.1.8. Respaldar la implementación de las acciones derivadas de auditorías, incidentes de seguridad de la información, análisis y tratamiento de riesgos, y demás oportunidades de mejora identificadas.

7.2. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO.

El Comité Institucional de Gestión y Desempeño, de conformidad con la normativa interna de la ALFM, constituye la instancia de coordinación y seguimiento para los sistemas de gestión institucionales, incluyendo el Sistema de Gestión de Seguridad de la Información.

En el marco del SGSI, le corresponde:

7.2.1. Revisar el estado de implementación, operación y desempeño del Sistema de Gestión de Seguridad de la Información (SGSI), de acuerdo con los informes y resultados presentados.
7.2.2. Analizar los resultados de los indicadores estratégicos de seguridad de la información y evaluar el cumplimiento de las metas establecidas.
7.2.3. Analizar los resultados y hallazgos de las auditorías internas y externas relacionadas con el SGSI, y realizar seguimiento a las acciones derivadas de estos.
7.2.4. Revisar el estado de los riesgos estratégicos de seguridad de la información y las acciones establecidas para su tratamiento.
7.2.5. Realizar seguimiento al cumplimiento de las actividades y metas establecidas en el Plan Estratégico de Seguridad y Privacidad de la Información (PESI).
7.2.6. Participar en la toma de decisiones y establecer las acciones que correspondan para el fortalecimiento y mejora del SGSI, de acuerdo con sus competencias.
7.2.7. Promover la articulación del SGSI con el Sistema Integrado de Gestión y con las políticas y lineamientos del Modelo Integrado de Planeación y Gestión (MIPG).

7.3. RESPONSABLE SEGURIDAD DE LA INFORMACIÓN.

El Responsable Seguridad de la Información es el encargado de diseñar, ejecutar y evaluar la implementación, operación, mantenimiento, seguimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), actuando como articulador entre la Alta Dirección, los líderes de proceso y las demás dependencias de la ALFM para garantizar la adecuada gestión de la seguridad de la información.

En el ejercicio de sus funciones, le corresponde:

7.3.1. Ejecutar las actividades relacionadas con la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), de acuerdo con los lineamientos establecidos.

7.3.2. Participar en el diseño, ejecución y seguimiento del Plan Estratégico de Seguridad y Privacidad de la Información (PESI), de acuerdo con las actividades y responsabilidades asignadas.

7.3.3. Apoyar la implementación y verificar el cumplimiento de la Política de Seguridad de la Información y demás lineamientos establecidos por la entidad.

7.3.4. Realizar la identificación, análisis, evaluación y seguimiento al tratamiento de los riesgos de seguridad de la información, de acuerdo con la metodología establecida.

7.3.5. Realizar las actividades requeridas para la actualización y mantenimiento del inventario de activos de información, de acuerdo con los lineamientos establecidos.

7.3.6. Apoyar a los líderes de proceso en la implementación y aplicación de los controles de seguridad de la información, de acuerdo con los lineamientos y procedimientos establecidos.

7.3.7. Realizar seguimiento al cumplimiento de los objetivos, metas e indicadores establecidos para el SGSI y reportar los resultados correspondientes.

7.3.8. Ejecutar las actividades de sensibilización, capacitación y fortalecimiento de la cultura de seguridad de la información, de acuerdo con los programas y planes establecidos.

7.3.9. Realizar el seguimiento a la atención y gestión de los incidentes de seguridad de la información, en articulación con las dependencias competentes y de acuerdo con los procedimientos establecidos.

7.3.10. Elaborar los informes relacionados con la gestión, implementación y desempeño del SGSI, para su presentación a las instancias correspondientes.

7.3.11. Participar en la revisión y actualización de las políticas, procedimientos, lineamientos y demás documentos que conforman el SGSI, de acuerdo con las necesidades identificadas y la normativa aplicable.

7.3.12. Apoyar la preparación y atención de auditorías internas y externas relacionadas con el SGSI, mediante la recopilación y organización de la información y evidencias requeridas.

7.3.13. Realizar seguimiento al cumplimiento de los planes de tratamiento de riesgos y de las acciones de mejora relacionadas con seguridad de la información, y reportar los avances correspondientes.

7.4. OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.

La Oficina de Tecnologías de la Información y las Comunicaciones es responsable de administrar y proteger la infraestructura tecnológica que soporta los procesos institucionales, implementando los controles técnicos necesarios para garantizar la seguridad de la información.

En el marco del SGSI, le corresponde:

7.4.1. Implementar, administrar y mantener los controles tecnológicos de seguridad de la información definidos por la Entidad, de acuerdo con los lineamientos y procedimientos establecidos.
7.4.2. Administrar la infraestructura tecnológica de la Entidad, aplicando las medidas y configuraciones de seguridad establecidas para su protección y adecuado funcionamiento.
7.4.3. Administrar los mecanismos de autenticación, autorización y control de acceso a los sistemas y servicios tecnológicos, de acuerdo con los lineamientos de seguridad establecidos.
7.4.4. Implementar y mantener los mecanismos de respaldo, copias de seguridad y recuperación de la información, de acuerdo con las necesidades y procedimientos establecidos por la Entidad.
7.4.5. Implementar y mantener medidas de protección para las redes, servidores, estaciones de trabajo y demás componentes de la infraestructura tecnológica, de acuerdo con los controles de seguridad definidos.
7.4.6. Identificar, gestionar y realizar seguimiento a las vulnerabilidades y actualizaciones de seguridad de la infraestructura tecnológica, de acuerdo con los procedimientos y niveles de criticidad establecidos.
7.4.7. Apoyar la identificación, contención, atención, recuperación y documentación de los incidentes de seguridad de la información relacionados con la infraestructura y los servicios tecnológicos, en articulación con las dependencias competentes.
7.4.8. Mantener los registros y mecanismos de monitoreo, trazabilidad y generación de evidencias de los eventos asociados a la infraestructura y los servicios tecnológicos, de acuerdo con los requerimientos establecidos.
7.4.9. Incorporar requisitos de seguridad de la información en la implementación y mantenimiento de proyectos, soluciones y servicios tecnológicos, de acuerdo con los lineamientos establecidos.
7.4.10. Realizar la gestión técnica de los cambios que puedan afectar la seguridad de la información, verificando la aplicación de los controles y medidas de seguridad correspondientes.

7.5. LÍDERES DE PROCESO.

Los líderes de proceso son responsables de garantizar que las actividades bajo su responsabilidad se desarrollen conforme a los lineamientos establecidos en el SGSI, incorporando la gestión de la seguridad de la información en la operación de sus procesos.

Les corresponde:

7.5.1. Identificar y mantener actualizada la información relacionada con los activos de información asociados a su proceso, de acuerdo con los lineamientos establecidos.

7.5.2. Designar, cuando corresponda y de acuerdo con las disposiciones institucionales, a los propietarios y custodios de los activos de información asociados a su proceso, y facilitar el desarrollo de sus responsabilidades.
7.5.3. Participar en la identificación, análisis, valoración y tratamiento de los riesgos de seguridad de la información asociados a su proceso.
7.5.4. Implementar, aplicar y mantener los controles de seguridad de la información definidos para su proceso, de acuerdo con los lineamientos y procedimientos establecidos.
7.5.5. Velar por el cumplimiento de las políticas, procedimientos, controles y demás lineamientos de seguridad de la información aplicables a su proceso.
7.5.6. Reportar oportunamente los eventos e incidentes de seguridad de la información identificados en el desarrollo de las actividades de su proceso, de acuerdo con los mecanismos establecidos.
7.5.7. Participar en auditorías, revisiones, verificaciones y demás actividades de seguimiento relacionadas con la seguridad de la información de su proceso.
7.5.8. Implementar y realizar seguimiento a las acciones correctivas, preventivas y de mejora que sean asignadas a su proceso, dentro de los plazos establecidos.
7.5.9. Promover entre los servidores públicos, contratistas y demás colaboradores de su proceso el cumplimiento de las buenas prácticas y lineamientos de seguridad de la información.

7.6. PROPIETARIOS DE ACTIVOS DE INFORMACIÓN.

Los propietarios de los activos de información son los responsables funcionales de la información generada, utilizada o administrada en el desarrollo de los procesos institucionales.

En el marco del SGSI, les corresponde:

7.6.1. Identificar, validar y mantener actualizada la información correspondiente a los activos de información bajo su responsabilidad, de acuerdo con los lineamientos establecidos.
7.6.2. Determinar y mantener actualizada la clasificación de los activos de información bajo su responsabilidad, de acuerdo con los criterios y lineamientos institucionales establecidos.
7.6.3. Determinar los requisitos de confidencialidad, integridad y disponibilidad aplicables a los activos de información bajo su responsabilidad, de acuerdo con las necesidades del proceso y los lineamientos institucionales.
7.6.4. Autorizar, cuando corresponda y de acuerdo con sus competencias, el acceso a la información bajo su responsabilidad, atendiendo los criterios y mecanismos de control de acceso establecidos.
7.6.5. Participar en la identificación, análisis, valoración y tratamiento de los riesgos de seguridad de la información asociados a los activos bajo su responsabilidad.
7.6.6. Verificar que los controles de seguridad de la información aplicables a los activos bajo su responsabilidad se encuentren implementados y operen de acuerdo con los lineamientos establecidos.

7.6.7. Informar oportunamente los cambios, modificaciones o situaciones que puedan afectar la seguridad, clasificación, disponibilidad, integridad o confidencialidad de los activos de información bajo su responsabilidad.

7.7. CUSTODIOS DE ACTIVOS DE INFORMACIÓN.

Los custodios son responsables de administrar y proteger los activos de información que les sean asignados, aplicando los controles definidos por la Entidad y garantizando su adecuado manejo durante todo su ciclo de vida.

Les corresponde:

7.7.1. Implementar y mantener los controles de seguridad de la información definidos para los activos bajo su custodia, de acuerdo con los lineamientos y procedimientos establecidos.
7.7.2. Aplicar las medidas necesarias para garantizar el almacenamiento, procesamiento, transmisión, conservación y disposición segura de la información bajo su custodia, de acuerdo con los requisitos establecidos.
7.7.3. Mantener actualizados los registros, configuraciones, evidencias y demás información relacionada con los activos bajo su custodia, de acuerdo con los procedimientos establecidos.
7.7.4. Informar oportunamente los incidentes, vulnerabilidades, eventos o condiciones que puedan afectar la seguridad de los activos de información bajo su custodia, utilizando los canales establecidos.
7.7.5. Apoyar la realización de inventarios, verificaciones y demás actividades de control relacionadas con los activos de información bajo su custodia.
7.7.6. Aplicar las medidas de protección definidas para los activos de información y colaborar con el propietario del activo en su implementación y seguimiento, de acuerdo con las responsabilidades asignadas.

7.8. USUARIOS DE LA INFORMACIÓN (SERVIDORES PÚBLICOS Y CONTRATISTAS).

Los servidores públicos y contratistas que, en el ejercicio de sus funciones u obligaciones contractuales, tengan acceso a los activos de información de la Agencia Logística de las Fuerzas Militares, son responsables de cumplir los lineamientos establecidos en el Sistema de Gestión de Seguridad de la Información (SGSI) y de proteger la información a la que accedan o administren.

En el marco del SGSI, les corresponde:

7.8.1. Cumplir la Política de Seguridad de la Información, las políticas específicas, procedimientos, protocolos y demás lineamientos institucionales aplicables al desarrollo de sus funciones u obligaciones.

7.8.2. Utilizar la información, los sistemas de información y los recursos tecnológicos únicamente para el desarrollo de las funciones, actividades u obligaciones autorizadas por la Entidad.

7.8.3. Proteger la confidencialidad, integridad y disponibilidad de la información a la que tengan acceso, de acuerdo con su clasificación y los lineamientos establecidos.

7.8.4. Mantener bajo custodia y proteger las credenciales, mecanismos y demás elementos de autenticación asignados, evitando su divulgación, préstamo, transferencia o uso por parte de terceros.

7.8.5. Reportar oportunamente los incidentes, eventos, vulnerabilidades, pérdidas, accesos no autorizados o cualquier otra situación que pueda afectar la seguridad de la información, a través de los canales establecidos.

7.8.6. Participar en las actividades de capacitación, sensibilización y fortalecimiento de competencias en seguridad de la información programadas por la Entidad, cuando les sean requeridas.

7.8.7. Cumplir las disposiciones establecidas para la clasificación, acceso, uso, almacenamiento, transmisión, conservación y disposición de la información, de acuerdo con los lineamientos institucionales.

7.8.8. Utilizar de manera responsable y adecuada los activos de información y recursos tecnológicos asignados, evitando su uso indebido, deterioro, pérdida o acceso no autorizado.

7.8.9. Adoptar buenas prácticas de seguridad de la información y contribuir al fortalecimiento de la cultura institucional de seguridad en el desarrollo de sus actividades.

7.9. SUPERVISORES E INTERVENTORES DE CONTRATOS.

Los supervisores e interventores de contratos son responsables de verificar que los contratistas y proveedores cumplan los requisitos de seguridad de la información establecidos por la ALFM durante la ejecución de los contratos.

En el marco del SGSI, les corresponde:

7.9.1. Verificar el cumplimiento de las obligaciones contractuales relacionadas con la seguridad de la información, de acuerdo con las condiciones y requisitos establecidos en el contrato.

7.9.2. Verificar la inclusión y aplicación de los requisitos de seguridad de la información en los procesos contractuales, cuando corresponda, de acuerdo con los lineamientos institucionales.

7.9.3. Realizar seguimiento al cumplimiento de los acuerdos de confidencialidad y no divulgación, compromisos de seguridad y demás obligaciones relacionadas con la protección de la información a cargo de los contratistas.

7.9.4. Informar oportunamente los incumplimientos, eventos o situaciones que puedan afectar la seguridad de la información institucional y que sean identificados durante la ejecución contractual.

7.9.5. Reportar a las instancias competentes los riesgos o situaciones que puedan afectar la seguridad de la información asociados a los servicios, bienes o actividades contratadas, de acuerdo con los mecanismos establecidos.

7.9.6. Verificar, al finalizar los contratos, el cumplimiento de las disposiciones relacionadas con la devolución, transferencia, eliminación, conservación o disposición de la información institucional, de acuerdo con los requisitos establecidos.

7.10. PROVEEDORES Y TERCEROS.

Los proveedores y terceros que presten servicios a la ALFM y que, como parte de la ejecución de sus obligaciones, tengan acceso a información institucional o a los activos de información, deberán cumplir los requisitos de seguridad definidos por la Entidad.

En desarrollo de sus obligaciones deberán:

7.10.1. Cumplir las cláusulas, requisitos, controles y demás obligaciones de seguridad de la información establecidos en los contratos, convenios o acuerdos suscritos con la Entidad.

7.10.2. Proteger la confidencialidad, integridad y disponibilidad de la información institucional a la que tengan acceso, de acuerdo con su clasificación y las condiciones establecidas.

7.10.3. Implementar y mantener las medidas y controles de seguridad acordados para la prestación de los servicios, suministro de bienes o ejecución de las actividades contratadas.

7.10.4. Informar oportunamente a la Entidad sobre los incidentes, eventos, vulnerabilidades o situaciones de seguridad que puedan afectar la información, los sistemas o los servicios institucionales.

7.10.5. Facilitar y atender las actividades de seguimiento, verificación, auditoría o evaluación que la Entidad realice en materia de seguridad de la información, dentro del alcance y condiciones establecidos contractualmente.

7.10.6. Realizar, al finalizar la relación contractual, la devolución, transferencia, eliminación o disposición segura de la información institucional, de acuerdo con las instrucciones de la Entidad y las obligaciones contractuales aplicables.

7.10.7. Cumplir la normativa vigente en materia de protección de datos personales, seguridad de la información, derechos de autor, propiedad de la información y demás disposiciones legales y reglamentarias aplicables a la relación contractual.

7.11. OFICINA DE CONTROL INTERNO.

La Oficina de Control Interno, en ejercicio de sus funciones de evaluación independiente y de conformidad con la normatividad vigente, contribuye al fortalecimiento del Sistema de Gestión de Seguridad de la Información mediante la realización de auditorías internas y el seguimiento a la implementación de acciones de mejora.

En el marco del SGSI, le corresponde:

7.11.1. Incluir, de acuerdo con la metodología y criterios de priorización establecidos, la evaluación del SGSI en el Programa Anual de Auditoría Interna, con un enfoque basado en riesgos.

7.11.2. Evaluar, de manera independiente y objetiva, la conformidad y eficacia del SGSI frente a los requisitos de la NTC-ISO/IEC 27001:2022, la normativa aplicable y los lineamientos y documentos institucionales establecidos.

7.11.3. Comunicar los resultados, hallazgos y conclusiones de las auditorías relacionadas con el SGSI a la Alta Dirección y a los responsables de los procesos correspondientes.

7.11.4. Realizar seguimiento a la implementación y eficacia de las acciones correctivas derivadas de las auditorías relacionadas con el SGSI, de acuerdo con los procedimientos establecidos.

7.11.5. Formular recomendaciones orientadas al fortalecimiento del SGSI, en el marco de las funciones de evaluación independiente correspondientes a la Tercera Línea de Defensa.

7.11.6. Contribuir al mejoramiento continuo del SGSI mediante la evaluación independiente, la identificación de oportunidades de mejora y la formulación de recomendaciones, sin asumir responsabilidades propias de su implementación.

8. SANCIONES

El incumplimiento de las disposiciones establecidas en la presente Política General de Seguridad de la Información, así como de los lineamientos, procedimientos, estándares y demás documentos que conforman el Sistema de Gestión de Seguridad de la Información (SGSI), podrá dar lugar a la adopción de las acciones administrativas, disciplinarias, contractuales, civiles, fiscales o penales a que haya lugar, de conformidad con la Constitución Política, la legislación colombiana, la normatividad interna de la Agencia Logística de las Fuerzas Militares y las obligaciones derivadas de la relación jurídica aplicable.

Toda presunta vulneración a la presente Política deberá ser reportada y gestionada conforme a los procedimientos institucionales para la gestión de incidentes de seguridad de la información y, cuando corresponda, será puesta en conocimiento de las autoridades o dependencias competentes para la evaluación de las acciones a que haya lugar.

La determinación de las medidas aplicables se realizará teniendo en cuenta, entre otros aspectos:

La naturaleza de la conducta o del incumplimiento.

El nivel de afectación sobre la confidencialidad, integridad, disponibilidad o autenticidad de la información institucional.

El impacto generado sobre la operación, los servicios o los activos de información de la Entidad.

La existencia de dolo, culpa o reincidencia.

El incumplimiento de obligaciones legales, contractuales o institucionales.

Las evidencias obtenidas durante la investigación o el análisis del incidente.

Cuando los hechos puedan constituir una conducta disciplinaria, fiscal, penal o un delito informático, la ALFM adelantará las actuaciones correspondientes o dará traslado a las autoridades competentes, de conformidad con la normatividad vigente.

9. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

La Agencia Logística de las Fuerzas Militares realizará el seguimiento, medición, análisis y evaluación del desempeño del Sistema de Gestión de Seguridad de la Información (SGSI), con el propósito de verificar el cumplimiento de la presente Política General de Seguridad de la Información, el logro de los objetivos del SGSI, la eficacia de los controles implementados y la mejora continua del Sistema.

Para tal efecto, la Entidad establecerá indicadores, mecanismos de seguimiento y criterios de evaluación que permitan medir el desempeño del SGSI y apoyar la toma de decisiones por parte de la Alta Dirección y del Comité Institucional de Gestión y Desempeño.

Como mínimo, el seguimiento y evaluación del SGSI comprenderá los siguientes aspectos:

El cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información.

El comportamiento y análisis de los indicadores definidos para el SGSI.

El avance en la implementación y madurez del Modelo de Seguridad y Privacidad de la Información (MSPI).

El cumplimiento de las actividades establecidas en el Plan Estratégico de Seguridad y Privacidad de la Información (PESI).

El estado de implementación y seguimiento de los planes de tratamiento de riesgos de seguridad de la información.

El análisis de los incidentes de seguridad de la información, sus causas, tendencias y acciones implementadas.

El resultado de las auditorías internas y externas relacionadas con el SGSI.

El seguimiento al cumplimiento de los requisitos legales, regulatorios y contractuales aplicables.

El avance en la implementación de las acciones correctivas, preventivas y oportunidades de mejora.

El avance en la implementación de la Política de Gobierno Digital, Seguridad Digital y de los instrumentos de medición definidos por las autoridades competentes, incluyendo aquellos que hagan parte del Formulario Único de Reporte de Avance de la Gestión (FURAG) o de los mecanismos que lo sustituyan.

Los resultados del seguimiento y la evaluación del SGSI serán presentados periódicamente a la Alta Dirección y al Comité Institucional de Gestión y Desempeño, con el fin de apoyar la toma de decisiones, la asignación de recursos y la definición de acciones orientadas al fortalecimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

10. APROBACIÓN Y REVISIONES A LA POLÍTICA

La presente Política General de Seguridad de la Información entrará en vigor a partir de su aprobación por la Alta Dirección de la Agencia Logística de las Fuerzas Militares, mediante el acto administrativo o mecanismo institucional que corresponda, y será de obligatorio cumplimiento para todos los destinatarios definidos en el ámbito de aplicación de la presente política.

Con el propósito de garantizar su conveniencia, adecuación y eficacia frente a las necesidades institucionales y al contexto de la Entidad, la Política será objeto de revisión periódica y, cuando corresponda, de actualización, como parte del proceso de mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

La revisión de la presente Política se realizará, como mínimo, en las siguientes circunstancias:

Anualmente, con el fin de evaluar su vigencia, eficacia, pertinencia y el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información.

Cuando se presenten cambios en el contexto interno o externo de la Entidad, incluyendo modificaciones en la estructura organizacional, el direccionamiento estratégico, los procesos institucionales o las necesidades y expectativas de las partes interesadas.

Cuando se expidan nuevas disposiciones legales, regulatorias o normativas que impacten la gestión de la seguridad de la información, la ciberseguridad, la protección de datos personales, el Modelo de Seguridad y Privacidad de la Información (MSPI) o la Política de Gobierno Digital.

Cuando se presenten incidentes de seguridad de la información, vulnerabilidades, amenazas emergentes o eventos que evidencien la necesidad de fortalecer o modificar los lineamientos establecidos en la presente Política.

Como resultado de auditorías internas, auditorías externas, revisiones por la Dirección o evaluaciones de desempeño del SGSI, cuando se identifiquen oportunidades de mejora o desviaciones que requieran su actualización.

Cuando se produzcan cambios significativos en la infraestructura tecnológica, los sistemas de información, los servicios tecnológicos o la gestión de los activos de información, que puedan afectar el alcance o la eficacia del Sistema de Gestión de Seguridad de la Información.

Las modificaciones que se realicen a la presente Política deberán ser evaluadas, aprobadas y divulgadas conforme al procedimiento institucional para el control de la información documentada del Sistema Integrado de Gestión, garantizando que la versión vigente se encuentre disponible para todos los destinatarios de la presente Política.