EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

ISSFA

INSTITUTO DE SEGURIDAD SOCIAL
DE LAS FUERZAS ARMADAS

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Tabla de contenido

1. Antecedentes

El Instituto de Seguridad Social de las Fuerzas Armadas (ISSFA) administra y resguarda información relacionada con los afiliados, pensionistas y beneficiarios del sistema de seguridad social militar. Esta información es un activo estratégico para la institución, ya que su adecuada gestión garantiza la continuidad operativa y el cumplimiento de los principios de confidencialidad, integridad y disponibilidad (CID).

En cumplimiento de la normativa vigente, el ISSFA adopta la presente Política de Seguridad de la Información (PSI) con el objetivo de establecer directrices para la protección de los activos de información institucionales. Esta política se enmarca en las disposiciones del Esquema Gubernamental de Seguridad de la Información (EGSI v3.0), de cumplimiento obligatorio en las entidades del sector público, conforme lo establece el Acuerdo Ministerial No. 0003-2024 del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL).

Adicionalmente, la PSI del ISSFA se fundamenta en la siguiente normativa:

- Constitución de la República del Ecuador, que establece el derecho a la protección de la información y la privacidad.
- Ley de Seguridad Pública y del Estado, que regula la protección de los activos tecnológicos y científicos en el ámbito de la seguridad nacional.
- Ley Orgánica de Protección de Datos Personales, que establece principios para el tratamiento seguro de la información personal.
- Normas de Control Interno de la Contraloría General del Estado, en lo referente a seguridad de la información y administración de riesgos tecnológicos.
- Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 del Ministerio de Telecomunicaciones y de la Sociedad de la Información (Mintel), que expidió el Esquema Gubernamental de Seguridad de la Información – EGSI.
- Reglamento Interno del Comité de Seguridad de la Información del ISSFA, aprobado mediante Resolución N.º 25-01.3

El Comité de Seguridad de la Información (CSI) del ISSFA es el órgano responsable de facilitar la implementación de las iniciativas de seguridad de la información en la institución. Dentro de este marco, el Oficial de Seguridad de la Información (OSI) es el encargado de implementar y actualizar el Esquema Gubernamental de Seguridad de la Información EGSI, coordinar las acciones necesarias para el cumplimiento del EGSI y la mejora continua de la seguridad de la información.

La presente política establece los roles y responsabilidades que deben cumplir todos los funcionarios, militares, contratistas y proveedores que manejen información institucional, garantizando su protección ante amenazas internas y externas.

2. Objetivo de la Política

Establecer los roles, responsabilidades, alcance y usuarios que permitan al ISSFA garantizar la adecuada protección de todos sus activos de información y prevenir la materialización de riesgos que puedan afectar su confidencialidad, integridad y disponibilidad, asegurando el cumplimiento de la normativa vigente, la continuidad operativa y la prestación eficiente de sus servicios a los afiliados, pensionistas y beneficiarios.

3. Política de Seguridad de la Información

3.1. Descripción de la Política

Para el ISSFA es fundamental contar con una Política de Seguridad de la Información (PSI), ya que a través de este documento se establecen los objetivos, roles y responsabilidades de los usuarios, así como el alcance que permita el manejo de la información del ISSFA.

Esta política permite definir y aplicar las mejores prácticas de seguridad para garantizar la adecuada protección de los activos de información, minimizando los riesgos asociados a su uso, almacenamiento, procesamiento y transmisión. Asimismo, contribuye al cumplimiento de la normativa vigente, asegurando que la institución opere bajo un marco regulatorio alineado con el Esquema Gubernamental de Seguridad de la Información (EGSI v3.0) y demás disposiciones legales aplicables.

La máxima autoridad del ISSFA, junto con el Comité de Seguridad de la Información (CSI), asume el compromiso de implementar el Esquema Gubernamental de Seguridad de la Información (EGSI), con el propósito de establecer un marco de confianza en el ejercicio de sus funciones, garantizando la protección de la información institucional y fortaleciendo la gestión de riesgos de seguridad.

En este contexto, el sistema de gestión de seguridad de la información en el ISSFA busca reducir la probabilidad o el impacto de los riesgos identificados sobre los activos de información, aplicando un enfoque sistemático que permita mantener un nivel de exposición controlado y responder eficazmente a los principios de confidencialidad, integridad y disponibilidad.

De acuerdo con lo expuesto, esta política es de aplicación obligatoria para todo el personal militar, servidores públicos, contratistas, proveedores y demás partes interesadas que interactúen con los activos de información del ISSFA.

3.2. Declaración de los objetivos de seguridad de la información

El ISSFA establece los siguientes objetivos de seguridad de la información, alineados con su Plan Estratégico Institucional (PEI), con el propósito de garantizar la protección de los activos de información, minimizar los riesgos asociados y fortalecer la gestión de seguridad en la institución:

3.2.1. Objetivo 1: Fortalecer la cultura de seguridad de la información

Este objetivo se encuentra alineado al O.E 2. Incrementar el desarrollo profesional del talento humano, promoviendo una cultura organizacional basada en la seguridad de la información a través de programas de capacitación, sensibilización y adopción de buenas prácticas, reduciendo los incidentes derivados del factor humano y asegurando la correcta aplicación de los lineamientos del EGSI.

3.2.2. Objetivo 2: Gestionar los riesgos de seguridad de la información

Este objetivo se encuentra alineado al O.E 1. Reducir el déficit actuarial para contribuir a la sostenibilidad del régimen especial de seguridad social de Fuerzas Armadas, implementando un proceso continuo de gestión de riesgos de seguridad de la información, mediante la identificación, evaluación y mitigación de amenazas, asegurando la aplicación de controles adecuados y alineados con los lineamientos del EGSI.

3.2.3. Objetivo 3: Garantizar la satisfacción de los asegurados mediante una gestión efectiva de incidentes de seguridad de la información

Este objetivo se encuentra alineado al O.E.5. Incrementar la satisfacción de los asegurados en la concesión de las prestaciones y servicios de seguridad social militar, mediante la implementación de procesos de gestión de incidentes que aseguren la disponibilidad, integridad y continuidad de los servicios digitales ofrecidos a los asegurados.

3.2.4. Objetivo 4: Asegurar el cumplimiento normativo en seguridad de la información

Este objetivo se encuentra alineado al O.E 3. Incrementar el grado de innovación en la gestión institucional, implementando el Esquema Gubernamental de Seguridad de la Información (EGSI) y ejecutando auditorías periódicas, evaluación de cumplimiento y corrección de hallazgos.

3.2.5. Objetivo 5: Fortalecer la resiliencia operativa y la continuidad del negocio

Este objetivo se encuentra alineado al O.E 4. Incrementar la efectividad operacional de los procesos y servicios, implementando planes de continuidad del negocio y recuperación ante desastres que permitan garantizar la disponibilidad de los servicios críticos del ISSFA ante fallas tecnológicas, ataques cibernéticos o eventos de fuerza mayor.

3.3. Roles y Responsabilidades

Para garantizar la adecuada gestión y protección de los activos de información del ISSFA, se establecen los siguientes roles y responsabilidades:

3.3.1. Máxima Autoridad

La Dirección General del ISSFA, a través del Comité de Seguridad de la Información (CSI), es responsable de garantizar que la seguridad de la información sea gestionada adecuadamente en toda la institución, asegurando el cumplimiento de la presente política y de las normativas vigentes en materia de seguridad de la información.

3.3.2. Comité de Seguridad de la Información (CSI)

Es el organismo encargado de la planificación, implementación y supervisión de las estrategias de seguridad de la información en la institución. Sus principales responsabilidades son:

- Gestionar la aprobación de la política de seguridad de la información institucional por parte de la máxima autoridad de la Institución;
- Establecer el alcance del sistema de seguridad de la información en función de los objetivos institucionales;
- Emitir las guías específicas que permitan la implementación del EGSI;
- Gestionar la implementación, control y seguimiento de las iniciativas relacionadas a la seguridad de la información;
- Aprobar el Plan de Comunicación y Sensibilización de Seguridad de la Información, y disponer su ejecución a las áreas correspondientes, con el objetivo de difundir las estrategias y buenas prácticas de seguridad de la información dentro de la institución;
- Gestionar la aprobación del plan de respuesta para el manejo de incidentes de seguridad de la información por parte del Comité de Continuidad del Negocio (CCN);
- Coordinar la continuidad de la operación de los servicios y sistemas de información de la institución, frente a incidentes de seguridad de la información, bajo supervisión con el CCN;
- Gestionar los incidentes relativos a la seguridad de la información con nivel de impacto medio y alto, de acuerdo con la categorización interna de incidentes;
- Supervisar la implementación de controles específicos de seguridad de la información para los sistemas o servicios, con base al EGSI;
- Supervisar la ejecución del Plan de Contingencia de Tecnología de la Información (PCTI) y su mejora continua;
- Informar semestral, o cuando la situación amerite, a la máxima autoridad los avances de la implementación y mejora continua del EGSI;
- Disponer a la UATH el fomento de la cultura de seguridad de la información en la institución;
- Las demás que se encuentren determinadas en las leyes, reglamentos y/o acuerdos dictados por la autoridad competente y el ente rector.

3.3.3. Oficial de Seguridad de la Información (OSI)

El OSI es el responsable de la gestión operativa de la seguridad de la información en la institución, asesorando al CSI y garantizando que las medidas de seguridad sean implementadas de manera efectiva. Sus funciones incluyen:

- Gestionar la ejecución del PCTI con la UTIC y las áreas involucradas, para garantizar la continuidad de las operaciones institucionales;
- Elaborar el plan de respuesta para el manejo de incidentes de seguridad de la información de impacto bajo, medio y alto; a ser revisado por el CSI y aprobado por el CCN;
- Gestionar los incidentes de seguridad de la información de bajo impacto;
- Coordinar la gestión de incidentes de impacto medio a través del CSI;

- Coordinar la gestión de incidentes de impacto alto a través del CCN; además, gestionar su mitigación en colaboración con el Centro de Respuesta a Incidentes Informáticos (CSIRT) sectorial (Cociber) y/o nacional (EcuCERT);
- Elaborar y mantener actualizada la documentación esencial del EGSI, para lo cual deberá coordinar con las áreas respectivas;
- Realizar el análisis de riesgos que afectan a los activos y recursos de información frente a las amenazas identificadas;
- Informar semestralmente al CSI sobre los riesgos identificados en el Estudio de Gestión de Riesgos de Seguridad de la Información, el progreso en la implementación del EGSI, las acciones de mejora continua y cualquier alerta que pueda obstaculizar su correcta aplicación;
- Coordinar con las diferentes áreas que forman parte de la implementación del EGSI, la verificación, monitoreo y el control del cumplimiento de las normas, procedimientos políticas y controles de seguridad institucionales establecidos de acuerdo a las responsabilidades y al mencionado estudio de cada área;
- Elaborar la propuesta del Plan de Comunicación y Sensibilización de Seguridad de la Información; que deberá ser presentado al CSI para su aprobación;
- Será responsable de conservar toda la documentación generada durante la implementación, seguimiento y mejora continua del EGSI, debidamente organizada y consolidada;
- Previa la terminación de sus funciones el OSI realizará la entrega recepción de la documentación generada y de la transferencia de conocimientos propios de la institución adquiridos durante su gestión, al nuevo oficial; procedimiento que será supervisado por la UATH, para la eliminación de accesos y claves. En caso de ausencia, la información será entregada al CSI;
- Administrar y mantener actualizado el EGSI mediante la definición, implementación y supervisión de normas, políticas y controles de seguridad de la información. Asimismo, garantizar que los propietarios de los activos de información sean responsables de cumplir con las disposiciones y controles establecidos para su protección dentro de los procesos organizacionales;
- Servir como enlace con los organismos del sector de las Telecomunicaciones y de la Sociedad de la Información tanto públicos como privados, y personas naturales que puedan influir o impactar en la implementación del EGSI.

Las demás que se encuentren determinadas en las leyes, reglamentos y/o acuerdos dictados por la autoridad competente y el ente rector.

3.3.4. Unidad de Tecnología, Informática y Comunicaciones (UTIC)

La UTIC es responsable de la implementación técnica de las medidas de seguridad de la información en los sistemas y redes del ISSFA. Sus responsabilidades incluyen:

- Aplicar controles de acceso a los sistemas de información y administrar los privilegios de usuarios.
- Implementar mecanismos de respaldo y recuperación de la información.
- Monitorear y gestionar la infraestructura tecnológica para prevenir incidentes de seguridad.
- Garantizar la actualización de sistemas y la aplicación de parches de seguridad.

3.3.5. Funcionarios, personal militar, asegurados del ISSFA y terceros involucrados

Todos los funcionarios, personal militar, asegurados, contratistas y terceros con acceso a la información del ISSFA tienen la obligación de:

- Cumplir con la Política de Seguridad de la Información y demás normativas aplicables.
- Manejar la información con responsabilidad, asegurando su confidencialidad, integridad y disponibilidad.
- Reportar de manera inmediata cualquier incidente o vulnerabilidad de seguridad detectada.
- Participar en capacitaciones y programas de concienciación en seguridad de la información.

3.4. Alcance y usuarios

3.4.1. Alcance

Esta Política de Seguridad de la Información (PSI) establece los roles y responsabilidades, incluye la declaración de los objetivos alineados al Plan Estratégico Institucional (PEI), y define a los usuarios a quienes aplica, con el fin de garantizar la adecuada protección de todos los activos de información del ISSFA, incluyendo datos electrónicos, físicos y cualquier otro medio de almacenamiento o procesamiento de información. Abarca los sistemas, redes, plataformas tecnológicas y procesos operativos que manejen información institucional, asegurando el cumplimiento de los principios de confidencialidad, integridad y disponibilidad (CID).

La política es de aplicación obligatoria dentro del marco del Esquema Gubernamental de Seguridad de la Información (EGSI), conforme a lo establecido en el Acuerdo Ministerial No. 0003-2024, y su implementación es supervisada por el Comité de Seguridad de la Información (CSI) del ISSFA.

3.4.2. Usuarios

Son usuarios de esta política todas las personas que interactúan con los activos de información del ISSFA, incluyendo:

- Personal militar, servidores y trabajadores públicos del ISSFA.
- Contratistas, proveedores y consultores que manejen información institucional.
- Afiliados, pensionistas y beneficiarios en lo que respecta a sus datos personales en los sistemas del ISSFA.
- Cualquier entidad externa con acceso a la información del ISSFA, bajo regulaciones y acuerdos específicos.

El cumplimiento de esta política es obligatorio para todos los usuarios mencionados, quienes deben acatar sus disposiciones y contribuir activamente a la seguridad de la información en la institución.

3.5. Comunicación de la Política

La Política de Seguridad de la Información del ISSFA será difundida a todos los funcionarios, personal militar, contratistas y terceros con acceso a la información institucional. Su

comunicación se realizará a través de los canales y medios establecidos en el Plan de Comunicación y Sensibilización, garantizando su comprensión y aplicación en todos los niveles de la organización.

Para su difusión se emplearán medios como el portal web institucional, correo electrónico, boletines internos y capacitaciones, asegurando que todo el personal conozca sus responsabilidades en la protección de la información.

3.6. Excepciones y sanciones

La Política de Seguridad de la Información del ISSFA es de aplicación obligatoria para todo el personal, sin embargo, podrán existir excepciones que se encuentren determinadas en la ley. Cualquier excepción deberá ser aprobada por el Comité de Seguridad de la Información (CSI) y documentada formalmente, asegurando que no comprometa la confidencialidad, integridad y disponibilidad de la información institucional.

El incumplimiento de las disposiciones establecidas en esta política será considerado una falta disciplinaria y estará sujeto a sanciones conforme a la normativa interna del ISSFA, la Ley Orgánica del Servicio Público (LOSEP) y la Ley Orgánica de Personal y Disciplina de Fuerzas Armadas. Las sanciones podrán incluir desde llamados de atención y suspensión de accesos hasta medidas administrativas o legales, dependiendo de la gravedad de la infracción.

4. Glosario de términos

Término	Definición
Activo de información	*Cualquier elemento valioso para la organización que debe ser protegido contra accesos no autorizados, uso indebido, divulgación, modificación, destrucción o compromiso.*
Confidencialidad	*Propiedad de la información que garantiza que solo las personas autorizadas puedan acceder a ella.*
Disponibilidad	*Propiedad de la información que garantiza que los usuarios autorizados tengan acceso a los activos de información cuando los necesiten.*
Integridad	*Propiedad de la información que asegura su exactitud y confiabilidad, evitando alteraciones no autorizadas.*
Incidente de seguridad de la información	*Evento que compromete la confidencialidad, integridad o disponibilidad de la información institucional.*
Gestión de riesgos	*Proceso de identificación, análisis y mitigación de amenazas que pueden afectar la seguridad de la información.*
Política de Seguridad de la Información (PSI)	*Conjunto de lineamientos y directrices que establecen las reglas para la protección de la información institucional.*
Oficial de Seguridad de la Información (OSI)	*Responsable de administrar y mantener actualizado el EGSI.*
Comité de Seguridad de la Información (CSI)	*Órgano encargado del control y seguimiento de la aplicación del EGSI.*
Control de acceso	*Mecanismos implementados para restringir el acceso a la información solo a usuarios autorizados.*

Plan de continuidad del negocio (PCN)	*Estrategia que asegura la operatividad de los servicios críticos de la institución en caso de incidentes o desastres.*
Respaldo de información	*Copia de seguridad de los datos institucionales para su recuperación en caso de pérdida o corrupción.*
Usuario	*Funcionarios públicos y personal militar que laboran en la institución y utilizan cualquier tecnología de Información.*
Usuario Externo	*Todo personal que no forma parte directa de la institución, pero que, por motivos laborables y previa autorización, hace uso de alguna tecnología de información del Issfa.*

5. Documentos de referencia

Esta política se fundamenta en normativas, estándares y directrices que regulan la seguridad de la información en el ISSFA. A continuación, se detallan los documentos de referencia aplicables:

- Ley Orgánica de Protección de Datos Personales.
- Acuerdo Ministerial No. 0003-2024 - EGSI v3.0.
- Esquema Gubernamental de Seguridad de la Información (EGSI v3.0).
- Normas de Control Interno de la Contraloría General del Estado.
- Reglamento Interno del Comité de Seguridad de la Información (CSI) del ISSFA.
- Plan Estratégico Institucional (PEI) del ISSFA 2024-2025.

6. Firmas de responsabilidad

	Nombre/Cargo	Firma
Elaborado por:	Tnte. Robinson Carranza / Oficial de Seguridad de la Información	Firmado electrónicamente por: ROBINSON ISRAEL CARRANZA MARTINEZ
Revisado por:	Mayo. William López / Presidente del Comité de Seguridad de la Información	Firmado electrónicamente por: WILLIAM GONZALO LOPEZ HERNANDEZ
Supervisado por:	Crnl. Robert Vargas Borbua / Subdirector General del ISSFA	Firmado electrónicamente por: ROBERT BOLIVAR VARGAS BORBUA
Aprobado por:	Grab. José Fiallo / Director General del ISSFA	Firmado electrónicamente por JOSE IGNACIO FIALLO VASQUEZ

Control de versiones

Versión:	1.0
Fecha de la versión:	26-03-2025
Creado por:	Oficial de Seguridad de la Información (OSI) - ISSFA
Aprobado por:	Comité de Seguridad de la Información (CSI) - ISSFA
Nivel de confidencialidad:	Uso Interno

Historial de cambios

Versión	Fecha	Detalle del cambio
1.0	26/03/2025	Emisión inicial del documento