POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

(EGSI versión 3.0)

Dirección: Buenos Aires Oe1-53 y Av. 10 de Agosto
Código postal: 170402 / Quito-Ecuador
Teléfono: +593-2 294-7400
www.aviacioncivil.gob.ec

Contenido

1. ANTECEDENTES

La creciente dependencia de la información y los sistemas tecnológicos en la Dirección General de Aviación Civil (DGAC), tanto para el desarrollo de sus actividades internas como para su interacción con el Estado y los ciudadanos, ha hecho evidente la necesidad de establecer un marco integral para la gestión de la seguridad de la información.

En este contexto, la protección de la información se ha convertido en una prioridad, impulsada por la necesidad de:

- Preservar la Confidencialidad, integridad y disponibilidad, estos son los tres pilares de la seguridad de la información. La política busca asegurar que la información solo sea accesible para personas autorizadas, que no sea modificada, alterada o destruida sin autorización y que esté disponible cuando sea necesaria.
- Protección integral de los activos de información, la política busca proteger contra accesos no autorizados, alteraciones, pérdidas o destrucciones todos los activos de información que son los elementos que tienen valor para la Dirección General de Aviación Civil (DGAC), ya sean datos personales, información financiera, propiedad intelectual, etc., en todos sus formatos, sean físicos o digitales.
- Apoyo a la misión y objetivos, la seguridad de la información no es un fin en sí mismo, sino un medio para apoyar el cumplimiento de la misión y los objetivos estratégicos de la Dirección General de Aviación Civil (DGAC). La política busca garantizar que la información esté disponible y sea confiable para la toma de decisiones y la operación de la institución.
- Minimizar los riesgos, identificando y gestionando las vulnerabilidades y amenazas que puedan afectar los activos de información de la Institución.
- Identificar amenazas, vulnerabilidades, accesos no autorizados, perdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales e implementar las medidas adecuadas.
- Cumplimiento normativo, la política se enmarca en el cumplimiento de leyes, reglamentos y estándares técnicos que regulan la seguridad de la información, como el Esquema Gubernamental de Seguridad de la Información (EGSI), Ley Orgánica de Protección de Datos Personales y otras normas relevantes.
- Mantener la confianza de los grupos de interés, fortaleciendo la confianza de los ciudadanos, clientes y funcionarios en la gestión de la información por parte de la Dirección General de Aviación Civil (DGAC).
- Promover una cultura de seguridad, fomentando la conciencia y responsabilidad de todo el personal en relación con la seguridad de la información.

En respuesta a estas necesidades, la Dirección General de Aviación Civil (DGAC) ha decidido implementar una **Política de Seguridad de la Información** que sirva como guía y marco de referencia para todas las acciones relacionadas con la protección de la información. Esta política se alinea con la misión y visión de la Institución y busca garantizar la seguridad de la información en todas sus formas y procesos, involucrando a todo el personal y partes interesadas.

2. OBJETIVO DE LA POLÍTICA

Garantizar la protección integral de los activos de información de la Dirección General de Aviación Civil (DGAC), estableciendo un marco integral para la gestión de seguridad de la información, con el fin de preservar su Confidencialidad, Integridad y Disponibilidad, en apoyo al cumplimiento de su misión y objetivos estratégicos y en cumplimiento de la normativa legal y técnica aplicable.

3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

3.1. Descripción de la Política

La Política de Seguridad de la Información de la Dirección General de Aviación Civil (DGAC) es un documento fundamental que establece el marco normativo y estratégico para la gestión de la seguridad de la información, que busca proteger los activos de información de la Institución, apoyar el cumplimiento de los objetivos institucionales y cumplir con la normativa aplicable, estableciendo las directrices, principios y responsabilidades para la gestión de la seguridad de la información, garantizando la confidencialidad, integridad y disponibilidad de la información

- Directrices, principios y responsabilidades, la política establece qué se debe hacer, cómo se debe hacer y quién es responsable de hacerlo en relación con la seguridad de la información.
- Gestión integra, la política abarca todos los aspectos de la seguridad de la información, desde la identificación, protección y accesos de activos hasta la gestión de riesgos y la capacitación del personal.
- Apoyo a la misión y objetivos: La seguridad de la información es un medio para apoyar el cumplimiento de la misión y los objetivos institucionales, y la política busca garantizar que la información esté disponible y sea confiable para la toma de decisiones y la operación de la Institución.

3.2. Declaración de los objetivos de seguridad de la información

Objetivo 1: Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que se convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, a todo el personal de la institución.

Objetivo 2: 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 tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.

Objetivo 3: 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 Institución.

3.3. Roles y responsabilidades

3.3.1. Máxima Autoridad

- Responsabilidades:
  Aprobar la política de seguridad de la información y sus modificaciones, promover la difusión y el apoyo a la seguridad de la información dentro de la institución, implementar el Esquema Gubernamental de Seguridad de la Información, conformar la estructura de seguridad de la información institucional, con personal formado y experiencia en gestión de seguridad de la información, así como asignar los recursos necesarios.
  Además, deberá designar al interior de la Institución:
  1. Al Comité de Seguridad de la Información (CSI) y;
  2. Al Oficial de Seguridad de la Información (OSI).
- Rol: Liderazgo y compromiso con la seguridad de la información.

3.3.2. Comité de Seguridad de la Información

- Responsabilidades:
  1. Establecer los objetivos de la seguridad de la información, alineados a los objetivos institucionales.

2. Gestionar la implementación, control y seguimiento de las iniciativas relacionadas a seguridad de la información.
3. Gestionar la aprobación de la política de seguridad de la información institucional, por parte de la máxima autoridad de la Institución.
4. Aprobar las políticas específicas internas de seguridad de la información, que deberán ser puestas en conocimiento de la máxima autoridad.
5. Realizar el seguimiento del comportamiento de los riesgos que afectan a los activos y recursos de información frente a las amenazas identificadas.
6. Conocer y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto de acuerdo a la categorización interna de incidentes.
7. Coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios, con base al EGSI.
8. Promover la difusión de la seguridad de la información dentro de la institución.
9. Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad de la información.
10. El comité deberá reunirse ordinariamente de forma bimestralmente y extraordinariamente en cualquier momento previa convocatoria.
11. Informar semestralmente a la máxima autoridad los avances de la implementación y mejora continua del Esquema Gubernamental de Seguridad de la Información (EGSI).

- Rol: Garantizar y facilitar la implementación de las iniciativas de seguridad de la información en la institución; y ser el responsable del control y seguimiento en su aplicación.

3.3.3. Oficial de Seguridad de la Información

- Responsabilidades:
  1. Identificar y conocer la estructura organizacional de la institución.
  2. Identificar las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI.
  3. Implementar y actualizar del Esquema Gubernamental de Seguridad de la Información EGSI en su institución.
  4. Elaborar y coordinar con las áreas respectivas las propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la Información (EGSI).
  5. Elaborar, asesorar y coordinar con los funcionarios, la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas.
  6. Elaborar y coordinar el Plan de concienciación en Seguridad de la Información basado en el Esquema Gubernamental de Seguridad de la Información (EGSI), con las áreas involucradas que intervienen y en coordinación con el área de comunicación institucional.
  7. Fomentar la cultura de seguridad de la información en la institución, en coordinación con las áreas respectivas.
  8. Elaborar el plan de seguimiento y control de la implementación de las medidas de mejora o acciones correctivas, y coordinar su ejecución con las áreas responsables.
  9. Coordinar la elaboración de un Plan de Recuperación de Desastres (DRP), con el área de TI y las áreas clave involucradas, para garantizar la continuidad de las operaciones institucionales ante una interrupción.
  10. Elaborar el procedimiento o plan de respuesta para el manejo de los incidentes de seguridad de la información presentados al interior de la institución.
  11. Coordinar la gestión de incidentes de seguridad de la información con nivel de impacto alto y que no pudieran ser resueltos en la institución, a través del Centro de Respuestas a Incidentes Informáticos (CSIRT) sectorial y/o nacional.
  12. Coordinar la realización periódica de revisiones internas al Esquema Gubernamental de Seguridad de la Información – (EGSI), así como, dar seguimiento en corto plazo a las recomendaciones que hayan resultado de cada revisión.
  13. Mantener toda la documentación generada durante la implementación, seguimiento y mejora continua del EGSI, debidamente organizada y consolidada, tanto políticas, controles, registros y otros.

14. Coordinar con las diferentes áreas que forman parte de la implementación del Esquema Gubernamental de Seguridad de la Información, la verificación, monitoreo y el control del cumplimiento de las normas, procedimientos políticas y controles de seguridad institucionales establecidos de acuerdo a las responsabilidades de cada área.
15. Informar al Comité de Seguridad de la Información, el avance de la implementación del Esquema Gubernamental de Seguridad de la Información y mejora continua (EGSI), así como las alertas que impidan su implementación.
16. Previa la terminación de sus funciones el Oficial de Seguridad de la información realizará la entrega recepción de la documentación generada al nuevo Oficial de Seguridad de la información, y de la transferencia de conocimientos propios de la institución adquiridos durante su gestión, en caso de ausencia, al Comité de Seguridad de la Información; procedimiento que será constatado por la unidad de talento humano, previo el cambio y/o salida del oficial de seguridad de la información.
17. Administrar y mantener el EGSI mediante la definición de estrategias políticas normas y controles de seguridad, siendo responsable del cumplimiento el propietario de la información del proceso.
18. Actuar como punto de contacto del Ministerio de Telecomunicaciones y de la Sociedad de la Información.

- Rol: Responsable de la implementación y mejora continua del EGSI, así como el de coordinar las acciones del Comité de Seguridad de la Información en relación a la implementación y cumplimiento del Esquema Gubernamental de Seguridad de la Información.

3.3.4. Dirección de Tecnologías de la Información y Comunicación (TIC)

- Responsabilidad: Implementar y gestionar los controles de seguridad tecnológica que soportan los sistemas administrativos, técnicos desarrollados para la institución, protegiendo la información almacenada en la infraestructura tecnológica.
- Rol: Responsable de la seguridad técnica de la información.

3.3.5. Personal de la Institución

- Responsabilidad: Conocer, cumplir y hacer cumplir las reglas, lineamientos, usos, procesos y procedimientos de la política de seguridad de la información, así como asistir a las capacitaciones y tomar conocimiento de las comunicaciones en materia de seguridad.
- Rol: Todos son responsables de la seguridad de la información en el ámbito de sus funciones.

3.4. Alcance y usuarios

El alcance de la Política de Seguridad de la Información es amplio y abarca todos los aspectos relacionados con la información que la Dirección General de Aviación Civil (DGAC) utiliza para el desarrollo de sus actividades. Esto incluye:

- Toda la información: Independientemente de su formato (física, digital), su contenido, su origen (interna o externa), su nivel de clasificación (pública, confidencial, reservada) o su ubicación.
- Todos los activos de información: Equipos, sistemas, aplicaciones, bases de datos, documentos, archivos, etc., que se utilizan para crear, procesar, almacenar, transmitir o gestionar información.
- Todos los procesos: Gobernantes, sustantivos, adjetivos, de apoyo y de la cadena de valor de la institución que involucren el uso de información.
- Todas las ubicaciones: Donde se encuentren los activos de información o se realicen procesos que involucren información.

Usuarios de la Política de Seguridad de la Información:

Los usuarios de la Política de Seguridad de la Información son todas las personas que tienen relación con la información de la Dirección General de Aviación Civil (DGAC), ya sean internas o externas. Esto incluye:

- Personal de la institución: Funcionarios, empleados, directivos, etc., independientemente de su cargo o función.
- Terceros externos: Proveedores, contratistas, consultores, colaboradores, etc., que tengan acceso a información de la Dirección General de Aviación Civil (DGAC).
- Ciudadanía en general: En la medida en que interactúa con la información de la institución, por ejemplo, a través de servicios en línea o solicitudes de información pública.

Todos los funcionarios de la institución tienen la responsabilidad de conocer la Política de Seguridad de la Información, comprenderla, cumplirla y hacerla cumplir con los diferentes usuarios de la información, en el ámbito de sus funciones y relaciones con la institución.

3.5. Comunicación de la Política

La socialización de la presente política se enfocará en todo el personal de la Dirección General de Aviación Civil (DGAC), estará a cargo de la Dirección de Comunicación Social.

3.6. Excepciones y sanciones

3.6.1. Excepciones a la Política de Seguridad de la Información:

Las excepciones a la Política de Seguridad de la Información son solicitudes formales para desviarse de los estándares de seguridad establecidos, con un motivo y duración específicos. Estas solicitudes deben cumplir con los siguientes criterios:

- Ser presentadas de manera documentada y justificativa.
- Contener un análisis de riesgos que justifique la excepción y su impacto en la organización.
- Especificar el periodo de vigencia y la fecha de reevaluación para asegurar que sigan siendo válidas.
- Contar con la aprobación del Oficial de Seguridad de la Información (OSI) y de la Dirección correspondiente.

3.6.2. Sanciones por Incumplimiento de la Política de Seguridad de la Información

El incumplimiento de la Política de Seguridad de la Información podrá derivar en sanciones administrativas, conforme a la normativa interna y legal aplicable. En este sentido, se aplicará el siguiente procedimiento:

- El Oficial de Seguridad de la Información reportará las infracciones detectadas a la Unidad Administrativa de Talento Humano.
- Se realizará un análisis de la gravedad del incumplimiento y de sus posibles impactos.
- Dependiendo de la naturaleza de la infracción, se podrá aplicar desde una notificación formal hasta sanciones disciplinarias conforme a la normativa vigente.
- Se establecerá un mecanismo de seguimiento y mitigación para prevenir reincidencias

Las sanciones se aplican cuando se incumplen las políticas de seguridad. En el caso de detectar incumplimiento de la presente política, la unidad administrativa competente deberá notificar de manera inmediata al Oficial de Seguridad de la Información (OSI) sobre la transgresión de la Política de Seguridad establecida en este instrumento, así como de cualquier otra normativa conexa.

A tal efecto, el Oficial de Seguridad de la Información procederá a elaborar un informe detallado sobre el incumplimiento detectado. Dicho informe será remitido, a la Dirección de Administración de Talento Humano y a la máxima autoridad, para su conocimiento y fines pertinentes.

4. VIGENCIA Y REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La **Política de Seguridad de la Información** de la Dirección General de Aviación Civil, entrará en vigencia a partir de la fecha de su expedición.

La **Política de Seguridad de la Información** de la Dirección General de Aviación Civil, será revisada anualmente o cuando se produzcan cambios significativos institucionales, legales, tecnológicos, entre otros.

5. GLOSARIO DE TÉRMINOS

Término	Definición
OSI	*Oficial de Seguridad de la Información*
CSI	*Comité de Seguridad de la Información*
EGSI	*esquema Gubernamental de Seguridad de la Información para las instituciones de la APCID para preservar la integridad, disponibilidad y confidencialidad de la información*
Activos de información	*Cualquier elemento valioso para una organización que debe ser protegido del acceso no autorizado, uso, divulgación, modificación, destrucción o compromiso*
Riesgo	*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.*
Confidencialidad	*La información solo tiene que ser accesible o divulgada a aquellos que están autorizados, los controles orientados a la confidencialidad buscan prevenir la divulgación no autorizada de información sensible*
Integridad	*La información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros, los controles de integridad buscan proteger la exactitud y la integridad de los datos frente a alteraciones no deseadas o maliciosas*
Disponibilidad	*La información debe estar siempre accesible para aquellos que estén autorizados, los controles de disponibilidad buscan prevenir interrupciones o limitaciones en el acceso a la información, asegurando su disponibilidad continua.*
Usuario	*Parte interesada con acceso a los sistemas de información de la institución, como personal, clientes, proveedores.*

6. DOCUMENTOS DE REFERENCIA

- Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003
- Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)
- Resolución Nro. DGAC-DGAC-2024-0076-R de 24 de agosto de 2024, Reglamento Interno del Comité de Seguridad de la Información (CSI) de la dirección General de Aviación Civil, conforme el Esquema Gubernamental de Seguridad de la Información (EGSI)

6. FIRMAS DE RESPONSABILIDAD

	Nombre / Cargo	Firma
ELABORADO POR:	Ing. José Luis Paredes **Especialista en Comunicaciones AFS1** **Oficial de Seguridad de la Información**	Firmado electrónicamente por: JOSE LUIS PAREDES SILVA Validar únicamente con FirmaEC
REVISADO POR:	Sr. William Giovanny Merino **Director de Planificación y Gestión Estratégica** **Presidente del Comité de Seguridad de la Información**	Firmado electrónicamente por: WILLIAM GIOVANNY MERINO SARANGO
	Sr. Ing. Manuel Alejandro Santana Mantilla **Director de Administración de Talento Humano**	Firmado electrónicamente por: MANUEL ALEJANDRO SANTANA MANTILLA
	Sr. Mgs. Oscar Ivan Jimenez Ramon **Director Administrativo**	Firmado electrónicamente por: OSCAR IVAN JIMENEZ RAMON
	Sra. Mgs. Robert Arturo Carrera Larco **Director de Comunicación Social**	Firmado electrónicamente por: ROBERT ARTURO CARRERA LARCO Validar únicamente con FirmaEC
	Sr. Ing. Juan Carlos Cárdenas Quenguán **Director de Tecnologías de la Información y Comunicación, Encargado**	Firmado electrónicamente por: JUAN CARLOS CARDENAS QUENGUAN Validar únicamente con FirmaEC
	Sra. Mgs. Andrea Pamela Aguilar Aguilar **Directora de Asesoría Jurídica**	Firmado electrónicamente por: ANDREA PAMELA AGUILAR AGUILAR Validar únicamente con FirmaEC
APROBADO POR:	Abg. Juan Pablo Franco **Director General de Aviación Civil, Encargado**	Firmado electrónicamente por: JUAN PABLO FRANCO CASTRO Validar únicamente con FirmaEC

CONTROL E HISTORIAL DE CAMBIOS

Versión	Descripción del Cambio	Fecha
1.0	Elaboración de la primera versión del documento	23/04/2020
1.1	Se realizan cambios en el numeral 2.5. Comunicación de la Política	19/04/2021
1.2	Se realizan cambios en el numeral 2.5. Comunicación de la Política	23/08/2022
1.3	Se realizan cambios en el numeral 2.5. Comunicación de la Política y numeral 3. Documentos de referencia. Se actualiza formato del documento	04/08/2023
2.0	Elaboración de la segunda versión del documento	18/02/2025