# “POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN FAC”

# POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## **LIDERAZGO Y COMPROMISO**

La Fuerza Aérea Colombiana a través del nivel estratégico, operacional y táctico deben liderar y demostrar compromiso mediante el cumplimiento de las siguientes actividades:

1. Asegurar que se establezca la política de seguridad y privacidad de la información y los objetivos de seguridad de la información y que sean compatibles con la misión y visión de la Institución.
2. Asegurar que los requisitos y controles del Sistema de Gestión de la Seguridad de la Información estén integrados a todos los procesos de la Institución.
3. Asegurar la disponibilidad de recursos necesarios para que el Sistema de Gestión de la Seguridad de la Información pueda llevarse a cabo según lo planeado.
4. Comunicar la necesidad de gestión de la seguridad de la información en la Institución y la necesidad de cumplir los requisitos del Sistema de Gestión de la Seguridad de la Información.
5. Asegurar que el Sistema de Gestión de la Seguridad de la Información logre los resultados previstos apoyando la implementación de todos los procesos de gestión de la seguridad de la información, y en particular solicitando y revisando informes sobre el estado y la eficacia del SGSI.
6. Dirigir y apoyar a los funcionarios de la Institución que están involucrados directamente con la seguridad de la información y el Sistema de Gestión de la Seguridad de la Información.
7. Hacer una valoración de las necesidades de recursos durante las revisiones realizadas, estableciendo objetivos para la mejora continua y seguimiento a la eficacia de las actividades planificadas.
8. Apoyar a las personas a las cuales se les han asignado roles y responsabilidades relacionadas con la gestión de la seguridad de la información.

## **POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

## **POLÍTICA GENERAL**

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la FAC con respecto a la protección de los activos de información (los funcionarios y terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Institución y apoyan la implementación del Sistema de Gestión de la Seguridad de la Información, por medio de la generación y publicación de sus políticas e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

## **POLÍTICAS ESPECIFICAS**

#### Política de uso aceptable (PUA).

La Fuerza Aérea Colombiana define, asigna y divulga a través del comité de seguridad de la información, los roles y responsabilidades de Seguridad de la Información, los cuales establecen actividades de administración, operación y gestión de la Seguridad de la Información, con el fin de implementar controles adecuados de seguridad, preservando la confidencialidad, integridad y disponibilidad de los activos propiedad de la FAC.

#### Organización de la Seguridad de la Información.

La Fuerza Aérea Colombiana define, asigna y divulga a través del comité de seguridad de la información, los roles y responsabilidades de Seguridad de la Información, los cuales establecen actividades de administración, operación y gestión de la Seguridad de la Información, con el fin de implementar controles adecuados de seguridad, preservando la confidencialidad, integridad y disponibilidad de los activos propiedad de la Institución.

#### Seguridad de los recursos humanos.

La Fuerza Aérea Colombiana identifica, define e informa a los funcionarios y terceros las responsabilidades y deberes que son asignadas a cada uno, asociadas con sus respectivos roles, para reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones y activos de información.

#### Gestión de activos de información.

La Fuerza Aérea Colombiana identifica, define y asigna las responsabilidades de protección para todos los activos de información, que garantice los niveles de seguridad, con el fin de mantener un inventario documentado con todas las propiedades, actualizado y exacto, clasificando los activos de acuerdo con la confidencialidad, integridad y disponibilidad.

#### Control de acceso lógico y físico.

La Fuerza Aérea Colombiana busca proteger la información, las áreas restringidas y los activos de información, contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico.

#### Dispositivos móviles, trabajo desde casa y BYOD

La Fuerza Aérea Colombiana a través de la presente política busca mitigar el riesgo en cuanto al uso inadecuado de dispositivos móviles y equipos de cómputo personales que accedan a la información o servicios de TI de la institución desde casa o desde las instalaciones de la FAC, con el fin de garantizar la confidencialidad e integridad de los datos que se envían y reciben a través de las redes.

#### Dispositivos de IoT

La FAC a través de la presente política busca mitigar los riesgos de seguridad de la información en cuanto al uso de los dispositivos de IoT que accedan a la información o servicios TI de la Institución, con el objetivo de garantizar la disponibilidad, confidencialidad y privacidad de la información que hace parte de la infraestructura tecnológica de la institución

#### Desarrollo Seguro.

La Fuerza Aérea Colombiana define las directrices para el desarrollo y mantenimiento seguro de todos los servicios, arquitectura, software, portales web y sistemas de información durante todo el ciclo de vida de desarrollo y mantenimiento de los sistemas de información, tanto en los nuevos desarrollos como en los cambios a los sistemas de información que sean desarrollados en la Institución o contratados con terceros.

#### Escritorio y pantalla limpios.

La Fuerza Aérea Colombiana establece la política de escritorio y pantalla limpios para prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral.

#### Transferencia de la Información.

La Fuerza Aérea Colombiana establece la política de transferencia de la información para prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en la plataforma tecnológica de la Institución.

#### Tratamiento y protección de datos personales.

La Fuerza Aérea Colombiana establece los lineamientos para el tratamiento y protección de datos personales, la cual se aplicará a todas las bases de datos y archivos que contengan datos personales y que sean objeto de tratamiento por parte de la Institución, considerado como responsable y encargado del tratamiento de los datos personales.

#### Aseguramiento del protocolo IPV6.

La Fuerza Aérea Colombiana define la política de seguridad para el aseguramiento del protocolo de seguridad en IPV6, con base a las características de confidencialidad, integridad y disponibilidad de la información, a fin de generar mecanismos de direccionamiento IP de acceso seguro y uso eficiente de la infraestructura tecnológica de la Institución.

#### Manejo de información, material e instalaciones que gozan de reserva legal.

De acuerdo con la ley de Inteligencia 1621 de 2013 y a la ley de Transparencia 1712 de 2014, la información que manejan ciertos organismos y entidades tienen reserva legal para proteger personas, organizaciones, medios, métodos entre otras, por tal razón la Fuerza Aérea Colombiana establece que la información que goza de reserva legal es la información clasificada y calificada.

#### Controles criptográficos.

La Fuerza Aérea Colombiana define los lineamientos de controles criptográficos encaminados a la protección de la información de la institución, con el fin de garantizar una adecuada protección de la confidencialidad, autenticidad e integridad de la información. Esta política aplica a todos las funcionarios y terceros que usen mecanismos criptográficos sobre los servicios o información de la Institución.

#### Respaldo de la Información.

La Fuerza Aérea Colombiana establece la política de respaldo de información para prevenir la pérdida de información crítica de la institución, salvaguardando de incidentes, daño o ataques que se encuentren en la plataforma tecnológica de la institución, soportando de esta manera la integridad, confidencialidad y disponibilidad de esta.

#### Relación con terceros.

La Fuerza Aérea Colombiana define los lineamientos para incluir los requisitos de seguridad necesarios para proteger los activos de información accesibles por terceros, incluyéndolos dentro de los acuerdos que se suscriban, por medio de un análisis que permita identificar los riesgos de seguridad de la información asociados para implementar planes de acción dependiendo del tipo de actividad con un tercero.

#### Seguridad en la nube.

La Fuerza Aérea Colombiana define los lineamientos para mantener la seguridad de los activos de la información cuando se autoriza el uso de servicios computacionales en la nube, a fin de garantizar la disponibilidad, privacidad, integridad y cumplimiento de los requisitos legales en materia de protección de información personal.

#### Uso de redes sociales.

La Fuerza Aérea Colombiana define los lineamientos para el uso de las redes sociales por parte de los miembros de la Institución, verificando el impacto que generan el uso de estas a nivel de la Seguridad Nacional y personal. Las redes sociales han revolucionado el concepto sobre las relaciones humanas, donde ya no es necesario un contacto físico, compartir una nacionalidad o el conocimiento de un mismo idioma, para relacionarse entre otros y compartir toda clase de información; ese flujo desbordado de información ha logrado, según el caso, impactar de manera positiva y negativa en aspectos políticos, sociales y económicos de distintas sociedades.

#### Gestión de incidentes de seguridad de la información.

La Fuerza Aérea Colombiana define los lineamientos para asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

#### Capacitación y sensibilización en seguridad de la información.

La Fuerza Aérea Colombiana define los lineamientos para la capacitación a funcionarios y terceros de la institución en cuanto a la seguridad de la información, para disminuir la cantidad de riesgos que se puedan presentar por vulnerabilidades al no contar con personal capacitado.

#### Aspectos de seguridad de la Información de la gestión de continuidad de negocio.

La Fuerza Aérea Colombiana define los lineamientos para determinar los requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas.

#### Cumplimiento.

La Fuerza Aérea Colombiana define los controles que permiten garantizar el cumplimiento con las políticas, normas y legislación aplicable, enfocándose principalmente en lo que se refiere a seguridad de la información.

## **ROLES Y RESPONSABILIDADES**

1. **Jefe Tecnologías de Información y Comunicaciones**

Tiene la responsabilidad de coordinar la administración, configuración de los recursos informáticos dentro de la plataforma tecnológica de seguridad, así como de gestionar la planificación y ejecución del plan de mantenimiento y actualización de la infraestructura tecnológica y de telecomunicaciones de la Institución y la implementación de las mejoras identificadas en la plataforma de seguridad que estén relacionadas con hardware, software, canales de comunicaciones de datos o infraestructura TI.

1. **Responsable de la gestión de servicios tecnológicos**
	* Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución.
	* Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información.
	* Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad.
	* Supervisar la respuesta a incidentes, así como la investigación de infracciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias.
	* Trabajar con la alta dirección y los responsables de los procesos misionales dentro de la Institución en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
	* Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
2. **Responsable de la Estrategia de TI**
	* Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la

seguridad de la información.

* + Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Encargado monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información.
1. **Responsable de los sistemas de Información**
	* Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la Institución.
	* Apoyar la implementación segura de los sistemas de información, de acuerdo con el Sistema de Gestión de Seguridad de la Información de la Institución.
	* Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
	* Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados.
	* Trabajar con la alta dirección y los responsables de los procesos misionales dentro de la Institución en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
2. **Comité de seguridad de la información**

El Comité de seguridad de la información debe asegurar que exista una dirección y apoyo por el alto mando para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en la Institución, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el Institución.

1. **Líderes de procesos Institucionales**

Se encargan de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el Sistema de Gestión de Seguridad de la Información al interior de su Institución, así como planear las actividades necesarias para una adecuada administración y sostenibilidad de este.

1. **Oficial del Sistema de Gestión de Seguridad de la Información (OSGSI)**

Es el responsable de implementar acciones para alinear la implementación del Sistema de Gestión de Seguirdad de la Información con los objetivos institucionales, así mismo define la normativa de seguridad y privacidad de la información y vela por su cumplimiento, previene, detecta y analiza las vulnerabilidades.

Interactúa directamente con la alta dirección para informar y reportar lo relacionado con la seguridad y privacidad de la información, da respuesta inmediata ante cualquier incidente de ciberseguridad y finalmente forma, concientiza y sensibiliza a la institución en materia de seguridad de la información.

Sus funciones y responsabilidades son ejecutadas desde el Comando de la Fuerza Aérea Colombiana, realiza coordinaciones y emite órdenes a los Oficiales de Seguridad de la Información, en los Comandos, Unidades Militares Aéreas, Grupos Aéreos, Escuelas de Formación, Club de Oficiales y Casino Central de Suboficiales.

1. **Oficial de Seguridad de La Información (OSI)**

El propósito del oficial de Seguridad de la Información es coordinar de manera permanente el proceso de implementación del Sistema de Seguridad de la Información a nivel Estratégico (Estado Mayor), Nivel operacional (03 Comandos), y nivel táctico (Unidades Militares Aéreas), así como asegurar el buen funcionamiento de la seguridad de los sistemas de información y de la aplicación y cumplimiento de las políticas de seguridad y privacidad de la información.

Se deberá nombrar al Oficial de Seguridad de la Información así; 01 en el nivel estratégico, 03 en el nivel táctico, 01 nivel táctico y/o por cada Unidad Militar Aérea.

1. **Responsable de la protección de los datos personales[[1]](#footnote-2)**

Es quien tiene decisión sobre las bases de datos que contengan este tipo de datos y que el responsable es quien direcciona las actividades de los encargados de los datos personales (quien realiza el tratamiento directamente), como se mencionaba anteriormente, adicional a las responsabilidades arriba citadas se tendrán en cuenta que de acuerdo a la Ley 1581 de 2012 Protección de Datos Personales los deberes y responsabilidades de los responsables y/o encargados del tratamiento de los datos personales son:

* Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.
* Tramitar las consultas, solicitudes y reclamos.
* Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran.
* Respetar las condiciones de seguridad y privacidad de información del titular.
* Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.
1. **Propietarios de activos de información.**
	* Definir el nivel de clasificación de la información, dar las directrices de uso del activo, autorizar privilegios y definir el ciclo de vida de este.
	* Informar a los Escuadrones de Telemática y/o quien haga sus veces, cuando detecte cualquier incidente de seguridad de la información, para que sea tratado y corregido mediante la aplicación de controles.
	* Implementar las medidas de seguridad de la información necesarias en su dependencia para evitar fraudes, robos o interrupción en los servicios o activos de información.
	* Asegurar que los funcionarios y/o terceros (proveedores, contratistas, pasantes, consultores entre otros.) que en cumplimiento a sus funciones tengan acceso a los activos de información institucional cumplan con las cláusulas de confidencialidad en los contratos y son conscientes de sus responsabilidades.
2. **Usuarios de la información**

Se entiendo por usuarios de la información a todos los funcionarios y terceros (proveedores, contratistas, pasantes, consultores entre otros.) que en cumplimiento a sus funciones tengan acceso a los activos de información institucional, estos deben:

* Conocer, comprender y aplicar las políticas de seguridad y privacidad de la información establecidas por la Fuerza Aérea Colombiana.
* Asegurar que sus acciones no afecten la seguridad de la información en la Institución.
* Comunicar oportunamente al Oficial de Seguridad de la Información (OSI), y/o Escuadrones de Telemática y/o quien haga sus veces, los incidentes de seguridad digital que detecte durante el desarrollo de sus actividades.
* Participar activamente en las campañas de sensibilización del SGSI.
1. Tomado de Guia No 4 Roles y Responsabilidades MINTIC [↑](#footnote-ref-2)