

**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD  
FINAGRO**

**PROCESO: ADMINISTRACIÓN DE RIESGOS**

**SUBPROCESO: ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN**

**TABLA DE CONTENIDO**

1. OBJETIVO .....	2
2. INTRODUCCIÓN .....	2
3. SEGURIDAD DE LA INFORMACIÓN .....	2
3.1 PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN.....	3
4. CIBERSEGURIDAD .....	4
4.2 PRINCIPIOS DE LA CIBERSEGURIDAD .....	4
5. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN .....	5
6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD .....	5
7. ALCANCE DE LA POLÍTICA.....	7
8. GOBIERNO CORPORATIVO .....	7
9. DIVULGACIÓN DE REPORTES DE GESTIÓN.....	8
10. COMPROMISO DE LA ALTA DIRECCIÓN.....	8
11. CUMPLIMIENTO DE LA POLÍTICA .....	9
12. ACTUALIZACIÓN DE LA POLÍTICA.....	9
13. IMPLEMENTACIÓN DE LA POLÍTICA .....	9
14. ANTECEDENTES NORMATIVOS .....	11

## **1. OBJETIVO**

Establecer las directrices, lineamientos, responsabilidades y conductas que seguirán todos los colaboradores de la Entidad para mantener los principios de confidencialidad, integridad, disponibilidad y privacidad de la información, desarrollando habilidades y conocimientos requeridos para tener y aplicar buenas prácticas de Seguridad de la Información y Ciberseguridad, de acuerdo con las necesidades de la Entidad y las normativas que apliquen.

## **2. INTRODUCCIÓN**

FINAGRO identifica la información como uno de los activos más importantes, ya que ésta se considera pilar para brindar sus servicios y cumplir con los objetivos propuestos. Información que se almacena, procesa y transporta en sistemas tecnológicos que soportan la operación de los diferentes procesos; siendo vital el servicio de la plataforma tecnológica para el funcionamiento de aplicaciones internas, externas, redes y en general equipos tecnológicos que se conectan entre sí en el ciberespacio para mantener la operación de la Entidad.

El presente documento describe la Política General de Seguridad de la Información y Ciberseguridad en FINAGRO, la cual se basa en estándares, buenas prácticas y normativas aplicables. La Política General de Seguridad de la Información y Ciberseguridad, definida y aprobada por la Junta Directiva es la base para definir la metodología de riesgos, implantación de controles y toma de decisiones de Seguridad de la Información y Ciberseguridad.

## **3. SEGURIDAD DE LA INFORMACIÓN**

Seguridad de la Información, es el conjunto de medidas que tienen como fin proteger y mantener los principios de confidencialidad, integridad y disponibilidad de los Activos de Información de FINAGRO, con el fin de prevenir incidentes tanto accidentales como intencionados, mediante la implementación de controles y medidas asociadas con las personas, los procesos y la tecnología, a la luz de las mejores prácticas y la alineación con los objetivos estratégicos de la Entidad, gestionando estrictamente el cumplimiento de obligaciones legales y regulatorias, fortaleciendo así la imagen y posición de FINAGRO.

La Seguridad de la Información se caracteriza por la preservación de:

- Su **Confidencialidad**, asegurando que sólo quienes estén autorizados puedan acceder a la Información.
- Su **Integridad**, asegurando que la Información y sus métodos de proceso sean exactos y completos.
- Su **Disponibilidad**, asegurando que los usuarios autorizados tengan acceso a la Información cuando lo requieran.

### 3.1 PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Con el fin de dar cumplimiento al marco normativo, regulatorio y a los objetivos de negocio, FINAGRO ha definido los siguientes **principios fundamentales** como soporte a la Política:

- La Información es uno de los activos más importantes de FINAGRO, y por tanto será utilizada acorde con los procesos del negocio, sus condiciones y regulaciones.
- La confidencialidad de la Información será mantenida, sin importar su medio, forma, sea física o digital o su estado, almacenada o en tránsito.
- La Información preservará su integridad independientemente de su ubicación, forma de almacenamiento y del canal de comunicación por el que sea transmitida.
- La Información estará disponible cuando sea requerida, en el formato y tiempo necesarios para una ejecución exitosa de las operaciones.
- FINAGRO velará por el cumplimiento de las regulaciones legales vigentes en materia de Seguridad de la Información que le apliquen.
- La privacidad de la Información de FINAGRO, de sus clientes, beneficiarios, contratistas, colaboradores y usuarios será preservada.
- Se mantendrá la trazabilidad de las acciones realizadas sobre la Información de negocio de FINAGRO durante el ciclo de vida de esta.
- En la Política de Administración de Datos Personales - ARI-DOC-023, se establecen las responsabilidades y roles tanto de FINAGRO como de los colaboradores en lo relacionado con el tratamiento de Datos Personales.

#### 4. CIBERSEGURIDAD

Ciberseguridad, es el conjunto de políticas, conceptos de seguridad, recursos, controles de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación, desarrollo, formación y buenas prácticas en general, utilizadas para prevenir y proteger los datos, sistemas y aplicaciones; salvaguardando a los consumidores financieros y activos de la Entidad en el ciberespacio, preservando los principios de la Seguridad de la Información e incluyendo las características de:

- **Control de accesos:** Proceso mediante el cual se permite o no el acceso de un usuario a aplicaciones, servidores, equipos tecnológicos entre otros, según los perfiles asignados. La política de control de acceso se encuentra detallada en las Políticas de Dominio de Seguridad de la Información y Ciberseguridad - ARI-DOC-015. Así mismo, en la Norma de Control de Accesos - ARI-DOC-018, se establecen los lineamientos detallados respecto al control de accesos, con el fin de evitar accesos no autorizados a los sistemas de información y plataformas tecnológicas.
- **No repudio:** Condición por medio de la cual no se puede negar la ejecución de una actividad realizada sobre la plataforma tecnológica, de acuerdo con los registros de auditoría o log's.

##### 4.1 PRINCIPIOS DE LA CIBERSEGURIDAD

Con el fin de dar cumplimiento al marco normativo, regulatorio y a los objetivos de negocio, FINAGRO considera los siguientes principios de la Ciberseguridad para preservar la información y correcto funcionamiento de la plataforma tecnológica para que no se afecten los procesos de la Entidad:

- **Mínimo privilegio:** Son todos aquellos privilegios que tienen los sistemas y aplicaciones que se encuentran interconectados pero que solo deben tener los usuarios, configuración y conexión de red necesarios para que funcionen de acuerdo con lo requerido por el proceso.
- **Mínima superficie de exposición:** Deben diseñarse las tareas o actividades a realizar en cada uno de los procesos de la Entidad, de tal forma que no queden o se habiliten canales, privilegios, IP's, usuarios, publicación o puertos que faciliten a un ciberdelincuente acceder a los sistemas, producto de estas debilidades de configuración en la red y plataforma tecnológica.

- **Defensa en profundidad:** Debe existir seguridad por niveles o anillos, es decir, que la arquitectura de red o controles de ciberseguridad que se implementen, tales como: firewall, IPS, IDS, Antivirus, WAF, antispam, honeypot, etc., deben configurarse en diferentes zonas de red. Así como usar diferentes dispositivos para dificultar el trabajo de un ciberdelincuente, obstaculizando su paso por las diferentes capas y evitando que cumpla con su objetivo.

## 5. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Los siguientes son los objetivos en materia de Seguridad de la Información y Ciberseguridad definidos por FINAGRO:

- Cumplir con las obligaciones legales vigentes relacionadas con Seguridad de la Información y Ciberseguridad que apliquen a la Entidad, tomando las medidas necesarias de acuerdo con la operación que se realiza en FINAGRO.
- Gestionar los riesgos de Seguridad de la Información y Ciberseguridad en todos los procesos de manera eficiente, con el fin de proporcionar continuidad y calidad a las operaciones del negocio.
- Facilitar la discusión al interior de la Entidad en temas de Seguridad de la Información y Ciberseguridad, ayudando a que todos los colaboradores, clientes y contratistas sean conscientes de las amenazas potenciales de Seguridad de la Información y Ciberseguridad con los riesgos asociados al negocio.
- Soportar y mejorar la calidad de las operaciones de FINAGRO, permitiendo un equilibrio entre funcionalidad y seguridad, a la luz de las mejores prácticas de la industria.

## 6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

FINAGRO, como el aliado estratégico para el desarrollo sostenible del Sector Agropecuario y Rural del país, a través de productos y servicios financieros que contribuyen a la generación de valor económico, social y ambiental que construyen la competitividad y sostenibilidad del sector, define sus procesos y brinda sus servicios de forma diligente y segura, generando confianza con los beneficiarios, Intermediarios Financieros, proveedores, colaboradores y demás grupos de interés o personas que

tienen relación con FINAGRO, administrando los recursos e información de forma segura.

Para FINAGRO, la información es considerada como uno de los activos importantes para el negocio y los procesos que soportan su operación, por este motivo se implementan buenas prácticas de Seguridad de la Información y Ciberseguridad que permiten cumplir con la normativa o requerimientos legales aplicables de los Entes de Control.

FINAGRO encamina los esfuerzos de los colaboradores y recurso técnico, para preservar la información y conservar la confidencialidad, integridad y disponibilidad de los activos de información, protegiendo y asegurando en el ciberespacio, los datos, sistemas y aplicaciones que son esenciales para la operación de la Entidad. Igualmente, FINAGRO se compromete a proteger los datos sensibles, ejecutando los procesos de manera óptima y manteniendo su privacidad.

Por tanto, FINAGRO debe:

- Establecer los fundamentos para el desarrollo y la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) y Ciberseguridad, que esté alineado con la estrategia corporativa y los objetivos del negocio.
- Definir los lineamientos y mejores prácticas que permitan la prevención, gestión y respuesta de incidentes de Seguridad de la Información y Ciberseguridad.
- Establecer que todos los colaboradores y terceros son responsables de registrar y reportar las violaciones y eventos sospechosos de Seguridad de la Información y Ciberseguridad, de acuerdo con los procedimientos correspondientes.
- Clasificar, proteger y asignar responsables de los Activos de Información, de acuerdo con la metodología que se establezca y con los criterios de valoración, en relación con la importancia que posee para la Entidad. Realizando igualmente el análisis de riesgos correspondiente, para definir los controles que preserven la información y plataforma tecnológica de la Entidad.
- Establecer los requisitos y buenas prácticas de Seguridad de la Información y Ciberseguridad, uso aceptable y controles relacionados con el acceso y utilización de los activos de la información de FINAGRO, que mantengan y protejan las características de confidencialidad, integridad y disponibilidad de éstos.
- Definir los lineamientos y mejores prácticas que permitan la prevención, gestión y respuesta de incidentes de Seguridad de la Información y Ciberseguridad de forma oportuna.

- Designar un equipo de Seguridad de la Información y Ciberseguridad, que se encargue de la guía, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, dando cumplimiento a la normativa.
- Definir las directrices y lineamientos relacionados con la gestión del recurso humano, para la concientización y pertenencia de la Seguridad de la Información y Ciberseguridad en todos los colaboradores.

## **7. ALCANCE DE LA POLÍTICA**

La Política General de Seguridad de la Información y Ciberseguridad, así como todos los documentos de apoyo al Sistema de Gestión de Seguridad de la Información, tienen alcance a toda la Entidad, incluyendo, pero no limitado a colaboradores temporales, pasantes, terceros, personal interno y externo que tenga algún vínculo con los procesos de la Entidad, o que por motivos de negocio tengan acceso a información de FINAGRO.

Quienes tengan acceso a la información deben adoptar los lineamientos definidos por Seguridad de la Información y Ciberseguridad, cumpliendo con las políticas, normas, procedimientos y/o estándares que hayan sido definidos.

## **8. GOBIERNO CORPORATIVO**

Para la aplicación y cumplimiento de la política, se establece el gobierno de Seguridad de la Información y Ciberseguridad, donde:

- La Junta Directiva Aprueba la Política General.
- El Presidente de FINAGRO y el Comité de Seguridad de la Información, aprueban las Políticas de Dominio.
- El Oficial de Seguridad de la Información, será el responsable de la gestión y estrategia para el cumplimiento y madurez de la Seguridad de la Información y Ciberseguridad en la Entidad.
- Los líderes de área deben asumir las responsabilidades que les sean asignadas para apoyar la ejecución de las Políticas de Dominio.
- Todos los colaboradores o comunidad FINAGRO deben cumplir con las políticas definidas.

## **9. DIVULGACIÓN DE REPORTES DE GESTIÓN**

Semestralmente el Oficial de Seguridad de la Información de la Entidad, presentará a la Junta Directiva y a la Alta Dirección los resultados de la gestión realizada frente a Seguridad de la Información y Ciberseguridad.

## **10. COMPROMISO DE LA ALTA DIRECCIÓN**

La Alta Dirección de FINAGRO en cabeza de su Presidente, reconoce la importancia de identificar y proteger los Activos de Información, así como la plataforma tecnológica que soporta los procesos de la Entidad, razón por la cual evidencia su compromiso con el Sistema de Gestión de Seguridad de la Información y Ciberseguridad, apoyando el desarrollo, implementación, formalización, mantenimiento y mejora continua, que permita la mitigación de los riesgos presentes en el ciberespacio, que lleguen a afectar los datos, sistemas y aplicaciones esenciales para la operación de la Entidad.

A su vez, la Alta Dirección fortalece su compromiso evidenciándolo a través de las siguientes actividades:

- Proporcionar los recursos adecuados para el mantenimiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.
- Promover la cultura de Seguridad de la Información y Ciberseguridad.
- Apoyar la divulgación de las políticas y demás lineamientos de Seguridad de la Información y Ciberseguridad.
- Revisar periódicamente el Sistema de Gestión de Seguridad de la Información y Ciberseguridad para aportar al mejoramiento continuo.
- Además, de todas aquellas actividades que se encuentran consignadas en la Circula Básica jurídica expedida por la Superintendencia Financiera de Colombia que apliquen a la Alta Dirección.

En caso de cualquier violación o incumplimiento a la Política, el Comité Directivo se ocupará de la situación adecuadamente y hará todo lo posible para resolver los incidentes, diagnosticar sus causas y evitar reiteraciones.

## **11. CUMPLIMIENTO DE LA POLÍTICA**

El cumplimiento de la Política de Seguridad de la Información y Ciberseguridad es obligatorio. Cada colaborador de planta, colaborador temporal, pasante, tercero, personal interno, personal externo y contratista de FINAGRO que tenga algún vínculo con los procesos o que acceda a la información o plataforma tecnológica de la Entidad, entenderá su rol y asumirá su responsabilidad respecto a los riesgos en Seguridad de la Información y Ciberseguridad, de acuerdo con las políticas definidas.

El incumplimiento de esta Política General podrá acarrear sanciones, de acuerdo con los procedimientos establecidos para tal fin en la Entidad.

## **12. ACTUALIZACIÓN DE LA POLÍTICA**

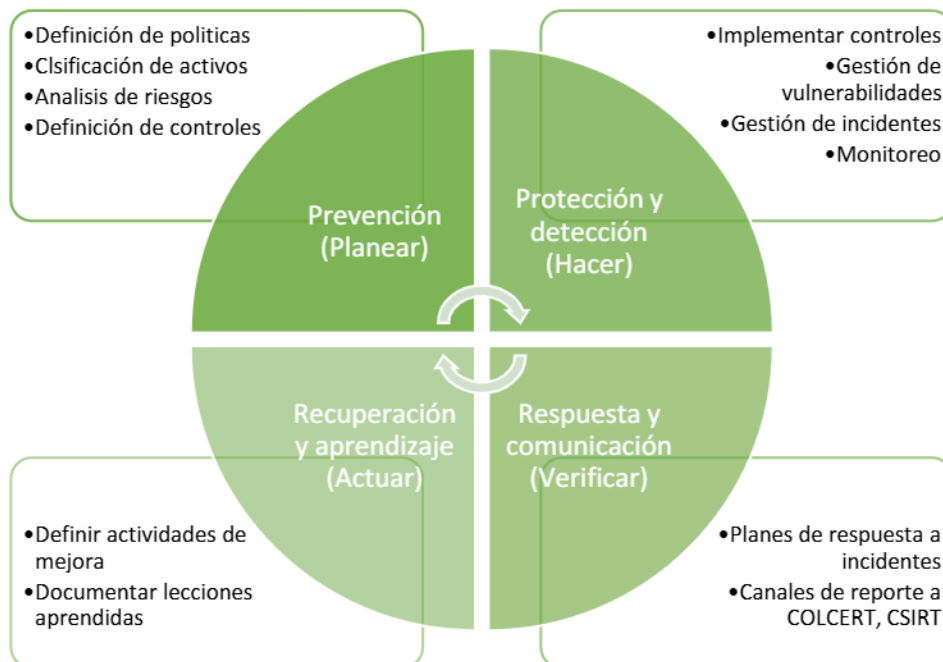
Se espera que la Política de Seguridad de la Información y Ciberseguridad se preserve en el tiempo, sin embargo, ante modificaciones por cambios en la regulación o marco legal aplicable, cambios estructurales que afecten a FINAGRO o incidentes graves, la política debe ser revisada y/o modificada y estos cambios aprobados por la Junta Directiva de FINAGRO.

## **13. IMPLEMENTACIÓN DE LA POLÍTICA**

La Política General de Seguridad de la Información y Ciberseguridad involucra el desarrollo e implantación de un Sistema de Gestión de Seguridad de la Información y Ciberseguridad integrado en el día a día de la operación de la Entidad. Como sistema de gestión, debe tener una madurez continua, para alcanzar los objetivos establecidos en el presente documento. Se anticipa y autoriza el desarrollo de *políticas de dominio, normas, procedimientos, estándares, guías, instructivos* que serán publicados en el aplicativo de Administración del SIG y otras medidas administrativas que sean necesarias incluyendo la definición de una unidad o grupo de Seguridad de la Información y Ciberseguridad, así como el desarrollo o la adquisición de las herramientas, software y demás recursos que se requiera como apoyo a la gestión realizada.

El Sistema de Gestión de Seguridad de la Información y Ciberseguridad se desarrolla con base en las siguientes etapas:

- **Prevención:** FINAGRO desarrolla e implementa controles para velar por la Seguridad de la Información y la gestión de la Ciberseguridad, que permiten evitar incidentes sobre la información o plataforma tecnológica.
- **Protección y detección:** FINAGRO implementa controles y actividades de monitoreo que permiten identificar eventos de Seguridad de la Información y Ciberseguridad, para tener una detección temprana que permita tomar acciones de contención o realizar la gestión que corresponda para atender los eventos evitando que estos se conviertan en incidentes.
- **Respuesta y comunicación:** FINAGRO establece planes de respuesta a incidentes de Seguridad de la Información y Ciberseguridad, para proceder a ejecutar actividades de análisis y contención, incluyendo la comunicación, en caso de ser necesario el apoyo de entes externos como por ejemplo el CSIRT del Gobierno o COLCERT.
- **Recuperación y aprendizaje:** FINAGRO define las actividades que permiten restaurar los servicios afectados por un incidente de Seguridad de la Información o Ciberseguridad, documentando posteriormente las lecciones aprendidas para identificar debilidades en controles, como se desarrolló el ataque, afectación y mejoras que puedan aplicarse a los planes de respuesta a incidentes.



#### **14. ANTECEDENTES NORMATIVOS**

El marco Normativo aplicable a FINAGRO en asuntos relacionados con Seguridad de la Información y Ciberseguridad, el cual es la base de la implementación del Sistema de Gestión se presenta a continuación:

- Circular Básica Jurídica de Superintendencia Financiera de Colombia.
- Ley 23 de 1993 y Ley 44 de 1993: Derechos de autor.
- Ley 679 de 2001 y Ley 1336 de 2009: Pornografía Infantil.
- Ley 1266 de 2008: Habeas Data.
- Ley 1273 de 2009: Delitos Informáticos.
- Ley 201 de 2012: Ley TLC.
- Ley 1581 de 2012: Protección de datos personales.
- Circular Externa 042 de 2012: Capítulo décimo segundo: Requerimientos mínimos de seguridad y calidad para la realización de operaciones.
- Circular Externa 007 de 2018: Requisitos mínimos para la gestión de riesgos de Ciberseguridad.