GERENCIA GENERAL

Resolución No. 002
Del 02 de marzo de 2026

Por la cual se adoptan la Política Institucional de Seguridad, Privacidad de la información; la Política Institucional de Tratamiento y Protección de Datos Personales; y la Política Institucional de Gestión de Incidentes de Seguridad de la Información y Datos Personales de la Federación Nacional de Cultivadores de Cereales, Leguminosas y Soya "Fenalce"

EL GERENTE GENERAL DE LA FEDERACIÓN NACIONAL DE CULTIVADORES DE CEREALES, LEGUMINOSAS Y SOYA – "FENALCE"

En uso de sus facultades legales estatutarias y legales, y

CONSIDERANDO

Que el inciso primero del artículo 15 de la Constitución Política Institucional de 1991, establece que "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".

Que la Ley 1273 de 2009 crea un nuevo bien jurídico tutelado denominado "De la protección de la información y los datos", preservando integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Que con fundamento en lo anterior, fue expedida la Ley Estatutaria 1581 de 2012 que tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma, estableciendo, además, las disposiciones generales para la protección de datos personales.

Que la Ley Estatutaria 1712 de 2014, define en su Artículo 1, que "el objeto de la presente ley es regular el derecho de acceso a la información

pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información."

Que el literal k) del artículo 17 de la Ley 1581 de 2012, establece como deber del responsable del tratamiento, la de adoptar Políticas Institucionales y procedimientos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos.

Que la Ley Estatutaria anteriormente señalada, fue reglamentada parcialmente por el Decreto 1377 de 2013.

Que en el marco del Decreto Nacional 2573 de 2014 establece los lineamientos generales de Gobierno en Línea e incorpora los requerimientos de la Ley 1581 de 2012 para la protección de datos personales y se diseñan en el marco de referencia a la norma ISO 27001 en cada uno de sus dominios.

Que el Decreto 1078 de 2015 dispone que las entidades que conforman la administración pública serán sujetos obligados para el cumplimiento de las Políticas y los lineamientos de la Estrategia de Gobierno en Línea, estableciendo en su artículo 2.2.9.1.2.1 como uno de sus cuatro componentes, el de la Seguridad y privacidad de la Información, comprendido por las acciones transversales a los componentes de TIC para Servicios, TIC para el Gobierno Abierto y TIC para la Gestión, tendientes a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.

Que el Decreto 103 de 2015 reglamenta parcialmente la ley de transparencia y el derecho de acceso a la información pública.

Que mediante el CONPES 3854 de 2016 el cual contiene la "POLÍTICA NACIONAL DE SEGURIDAD DIGITAL" se establecen los lineamientos y directrices de seguridad digital, incluyendo componentes tales como la gobernanza, educación, la regulación, la cooperación internacional y nacional, la investigación, el desarrollo y la innovación.

Que mediante el CONPES 3995 de 2020 el cual contiene la "POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL" formula una política nacional que tiene como objetivo, establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital.

Que el Decreto Nacional 1008 de 2018 establece el habilitador transversal de seguridad de la información como elemento fundamental para el logro de los propósitos de esta.

Que **LA FEDERACIÓN NACIONAL DE CULTIVADORES DE CEREALES, LEGUMINOSAS Y SOYA "FENALCE"**, recolecta, procesa, almacena y transfiere información en formato físico y digital. Esta información es un activo fundamental para el cumplimiento de la misión de la federación y proviene de diversas fuentes como agremiados, asociaciones, funcionarios, contratistas, proveedores y entidades públicas y privadas; por lo cual la gestión de dicha información requiere un manejo responsable y seguro, que permita realizar un buen uso de la misma y mitigar los riesgos sobre su confidencialidad, disponibilidad e integridad.

Que para lograr el buen uso y seguridad de la información, **LA FEDERACIÓN NACIONAL DE CULTIVADORES DE CEREALES, LEGUMINOSAS Y SOYA "FENALCE"**, requiere la implementación de un conjunto de controles, políticas institucionales, procesos, procedimientos, estructuras organizacionales y componentes de software y hardware. Esta implementación requiere desde la identificación de los activos de información y el análisis de riesgos, hasta establecer, implementar y hacer seguimiento continuo a dichos controles y su efectividad; razón por la cual se hizo necesario incorporar en el Sistema Integrado de Gestión de FENALCE, el Sistema de Gestión de Seguridad de la Información que permita identificar y gestionar dichos riesgos.

Que la Norma ISO/IEC 27001 y sus actualizaciones es la norma estándar para la seguridad de la información expedida por la Organización Internacional de Normalización.

Que **LA FEDERACIÓN NACIONAL DE CULTIVADORES DE CEREALES, LEGUMINOSAS Y SOYA "FENALCE",** por ser un ente privado no se regula en estricto sentido mediante la normatividad de la administración pública. Pero al ser administradores de los recursos provenientes de los Fondos Parafiscales de Fomento si precisa unificar los criterios que se requieran para el cumplimiento de los objetivos en sus programas y proyectos.

Que alineados con la Política de Gobierno Digital y teniendo en cuenta que la Norma ISO/IEC 27001 y sus actualizaciones es una norma emitida por la Organización Internacional de Normalización, que describe cómo gestionar la seguridad de la información en una organización, **LA FEDERACIÓN NACIONAL DE CULTIVADORES DE CEREALES, LEGUMINOSAS Y SOYA "FENALCE"** determina que la implementación del Sistema de Gestión de Seguridad de Información SGSI, se realice en el marco de dicha norma, sobre la cual se desarrolla la Política Institucional de Seguridad y Privacidad de la Información.

Que Política Institucional de Seguridad, Privacidad de la información, la Política Institucional de Tratamiento y Protección de Datos Personales, y la Política Institucional de Gestión de Incidentes de Seguridad de la

Información y Datos Personales, adoptadas mediante la presente resolución, fueron elaboradas por la Oficina de Sistemas y aprobadas por el Gerente General de FENALCE.

En mérito de lo expuesto,

RESUELVE

ARTÍCULO PRIMERO: Adoptar la Política Institucional de Seguridad y Privacidad de la Información, política que hace parte integral de la presente con el **CÓDIGO: IN-SI-007**.

ARTICULO SEGUNDO: Adoptar la Política Institucional de Tratamiento y Protección de Datos Personales, política que hace parte integral de la presente con el **CÓDIGO: IN-SI-008**.

ARTICULO TERCERO: Adoptar la Política Institucional de Gestión de Incidentes de Seguridad de la Información y Datos Personales, política que hace parte integral de la presente con el **CÓDIGO: IN-SI--009**.

ARTICULO CUARTO: Disponer la publicación de la presente resolución en la página web de la Federación, así como la socialización del presente acto al interior de FENALCE. Para tales efectos, se designa a la Oficina de Sistemas como responsable de coordinar la publicación, divulgación y socialización institucional de la presente resolución y de las Políticas adoptadas.

ARTICULO QUINTO: La presente Resolución rige a partir de su publicación interna y externa, según corresponda, y deroga las disposiciones anteriores que le sean contrarias.

ARTÍCULO SEXTO: La Oficina de Sistemas, en articulación con las dependencias competentes, deberá adelantar la implementación progresiva de los procedimientos, formatos, matrices, controles y demás instrumentos operativos requeridos para la aplicación efectiva de las políticas adoptadas mediante la presente resolución.

Dada en Cota, Cundinamarca, a los dos (02) días del mes de marzo de 2026.

ARNULFO TRUJILO DIAZ
GERENTE GENERAL

POLÍTICA INSTITUCIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

(En cumplimiento de la Ley Estatutaria 1581 de 2012 y normas concordantes)

1. OBJETO

La Federación Nacional de Cultivadores de Cereales, Leguminosas y Soya – FENALCE, establece la presente Política de Seguridad y Privacidad de la Información con el fin de definir las normas, principios y compromisos institucionales orientados a garantizar la confidencialidad, integridad y disponibilidad de la información que es obtenida, generada, procesada, almacenada o transmitida en el desarrollo de su misión.

Esta política constituye el marco de referencia para la implementación, operación, mantenimiento y mejora continua de la gestión de la seguridad y privacidad de la información en FENALCE, implementada de forma proporcional al tamaño, naturaleza y recursos de la Federación, tomando como referencia buenas prácticas internacionales (incluida ISO/IEC 27001) sin implicar la adopción integral de modelos de gestión propios de entidades públicas, salvo en aquello que resulte pertinente al contexto gremial de la Federación.

2. Alcance

La presente política aplica a:

- Toda la información obtenida, generada, tratada, almacenada o transmitida por FENALCE, en cualquier formato (físico, digital, verbal o audiovisual).

- Todos los activos que soportan la información: sistemas de información, infraestructura tecnológica, dispositivos, redes, aplicaciones, servicios en la nube, repositorios y documentos físicos.

- Todos los funcionarios, contratistas, proveedores, aliados estratégicos, visitantes y terceros que, en virtud de su relación con FENALCE, tengan acceso a información institucional.

3. Marco institucional y normativo

La política se encuentra alineada con:

- La misión y objetivos institucionales de FENALCE.

- La normatividad vigente aplicable en Colombia en materia de seguridad de la información, seguridad digital y protección de datos personales, en especial la Ley 1581 de 2012, el Decreto 1377 de 2013 y el Decreto Único Reglamentario 1074 de 2015, así como directrices de la Superintendencia de Industria y Comercio (SIC).

- Referentes, estándares y buenas prácticas reconocidas en materia de seguridad y privacidad de la información, tales como: i) guías y lineamientos expedidos por entidades competentes en Colombia (por ejemplo, MinTIC y SIC, en la medida en que resulten aplicables a entidades privadas), y ii) estándares internacionales, incluyendo ISO/IEC 27001 y normas afines, tomados como referencia para la mejora continua de la gestión de seguridad de la información.

4. Articulación con documentos institucionales relacionados

La presente política se complementa y desarrolla mediante los siguientes documentos institucionales:

- Política de Tratamiento de Datos Personales de FENALCE, que define las finalidades de tratamiento, derechos de los titulares, procedimientos de consultas y reclamos, lineamientos de seguridad de datos personales, gestión de incidentes y obligaciones de responsables y encargados.

- Procedimiento de Gestión de Seguridad de la Información y Protección de datos, que establece el marco operativo para la gestión de riesgos, clasificación de información, controles de seguridad, control de accesos, copias de respaldo, gestión de incidentes, auditoría y mejora continua.

El cumplimiento de esta política implica la adopción y cumplimiento de estos documentos, sus actualizaciones y los procedimientos específicos asociados.

5. Principios de seguridad y privacidad de la información

FENALCE adopta los siguientes principios como base de su gestión de seguridad y privacidad de la información:

- Confidencialidad: la información solo será accesible a personas debidamente autorizadas.
- Integridad: la información será protegida contra modificaciones no autorizadas o accidentales.
- Disponibilidad: la información estará disponible cuando sea requerida por los usuarios autorizados.
- Legalidad: el tratamiento de la información se realizará conforme a la normativa vigente.
- Responsabilidad: cada usuario es responsable del uso adecuado de la información bajo su custodia.
- Mejora continua: los controles y medidas de seguridad serán evaluados y actualizados periódicamente.

6. Enfoque de gestión de riesgos de seguridad de la información

FENALCE gestionará la seguridad y privacidad de la información con un enfoque basado en riesgos, proporcional a su naturaleza gremial y a sus capacidades técnicas y financieras.

- Se identificarán y priorizarán los activos de información críticos para el cumplimiento de la misión, la operación de los servicios y la protección de los datos personales de los titulares vinculados a FENALCE.
- Periódicamente se evaluarán los riesgos de seguridad de la información asociados a dichos activos, estableciendo tratamientos razonables y viables (controles organizacionales, técnicos, físicos y contractuales) acordes con la realidad de la Federación.

7. Compromiso de la alta dirección

La alta dirección de FENALCE manifiesta su compromiso expreso con:

- Promover una cultura institucional de seguridad y privacidad de la información.

- Asegurar el cumplimiento de los requisitos legales, normativos, contractuales y regulatorios aplicables.

- Asignar recursos humanos, técnicos y financieros necesarios para implementar, mantener y mejorar la seguridad y privacidad de la información.

- Garantizar la gestión del riesgo de seguridad de la información, incluyendo la identificación, valoración, tratamiento y seguimiento de riesgos.

- Respaldar la gestión de auditorías internas, revisiones de cumplimiento y planes de mejora.

- Asegurar la adecuada gestión de incidentes de seguridad de la información y de privacidad, incluyendo la atención de eventos que puedan afectar datos personales, con su debido análisis y notificación cuando aplique conforme Política de Tratamiento de Datos Personales.

8. Roles y responsabilidades

FENALCE definirá y asignará roles y responsabilidades relacionadas con la seguridad y privacidad de la información, incluyendo, entre otros:

8.1. Gerencia General

- Liderar y apoyar la adopción de la presente política.

- Aprobar y priorizar recursos para la gestión de seguridad y privacidad de la información.

- Velar por el cumplimiento institucional de esta política.

- Asegurar que la implementación de controles de seguridad de la información sea proporcional a los riesgos identificados y a los recursos disponibles, priorizando los activos y procesos más críticos para FENALCE.

8.2. Junta Directiva

- Conocer la política y sus actualizaciones, así como los reportes de riesgos, incidentes y planes de mejora.

8.3. Oficial de Seguridad de la Información (OSI)

- Coordinar la implementación y mejora continua de la gestión de la seguridad y privacidad de la información.
- Liderar y acompañar la gestión de riesgos de seguridad de la información.
- Supervisar el cumplimiento de controles técnicos y organizacionales.
- Coordinar la respuesta a incidentes y asegurar la documentación de los eventos.

8.4. Oficial de Protección de Datos Personales (OPD)

- Administrar el cumplimiento de la Política de Tratamiento de Datos Personales y de las obligaciones asociadas al tratamiento de datos personales.
- Coordinar la atención de consultas y reclamos (Habeas Data).
- Coordinar, cuando aplique, notificaciones a la Superintendencia de Industria y Comercio (SIC) en caso de incidentes que comprometan datos personales.

8.5. Área de Tecnología

- Administrar la infraestructura tecnológica, controles de seguridad, accesos, respaldos, monitoreo y disponibilidad de servicios.
- Implementar controles técnicos aprobados y recomendaciones derivadas del análisis de riesgos.
- Proponer soluciones y controles de seguridad viables técnica y económicamente, priorizando medidas de alto impacto y bajo costo

(por ejemplo, gestión de credenciales, copias de respaldo, actualizaciones, protección contra malware y registro básico de eventos).

- Apoyar al OSI y al OPD en el manejo de incidentes y evidencias técnicas.

8.6. Líderes de Proceso y Responsables de Activos de Información

- Identificar y reportar activos de información en su proceso.
- Garantizar la clasificación y custodia de la información bajo su responsabilidad.
- Asegurar la aplicación de medidas organizacionales y controles definidos.

8.7. Usuarios, contratistas y terceros

- Cumplir la presente política y los procedimientos asociados.
- No divulgar información sin autorización.
- Reportar oportunamente incidentes o sospechas de vulnerabilidad.
- Aplicar prácticas seguras en el uso de herramientas y credenciales.

9. Lineamientos generales de seguridad de la información

FENALCE implementará, de manera gradual y priorizada, controles técnicos y organizacionales al menos para:

- La clasificación de la información según su nivel de sensibilidad (pública, de uso interno, restringida, confidencial), definiendo reglas básicas de tratamiento y divulgación para cada categoría.
- El control de accesos y administración de credenciales con el principio de mínimo privilegio, autenticación individual y prohibición de compartir usuarios y contraseñas.

- La protección contra pérdida, alteración o acceso no autorizado, incluyendo como mínimo: uso de software de seguridad, actualización periódica de sistemas y aplicaciones, así como bloqueo de equipos cuando no estén en uso.

- La ejecución de copias de respaldo periódicas de la información crítica y la verificación básica de su restauración, con responsabilidades definidas para su custodia.

- La gestión de terceros que accedan a información o sistemas de FENALCE, incorporando cláusulas de confidencialidad y de seguridad de la información en contratos y convenios cuando aplique.

10. Gestión de incidentes de seguridad y privacidad

Toda persona vinculada a FENALCE debe reportar inmediatamente cualquier incidente o sospecha que afecte o pueda afectar la seguridad y privacidad de la información.

Los incidentes serán gestionados conforme al Procedimiento de Gestión de Seguridad de la Información y Protección de Datos, incluyendo su análisis, contención, erradicación, recuperación, registro y lecciones aprendidas.

Cuando un incidente involucre datos personales, se aplicarán los lineamientos establecidos en la POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES, incluyendo las acciones de notificación y comunicación que sean requeridas por ley o por directrices de la SIC.

11. Gobierno y aprobación

Los temas relacionados con seguridad de la información y seguridad digital serán incluidos en la agenda de la Junta Directiva de FENALCE.

La presente política deberá ser:

- Revisada y aprobada por la Gerencia General.
- Formalizada mediante acta.
- Expedida por la máxima autoridad de la entidad, el Gerente General.

12. Comunicación, cumplimiento e indicadores básicos

FENALCE comunicará esta política a todos los funcionarios, contratistas y terceros según corresponda, y realizará acciones de sensibilización y formación para promover una cultura de seguridad y privacidad.

El incumplimiento de esta política podrá generar acciones administrativas, disciplinarias, contractuales o legales, según corresponda y conforme a los compromisos adquiridos por cada parte.

Como parte de las actividades de seguimiento, FENALCE podrá definir y monitorear indicadores sencillos de seguridad de la información (por ejemplo, número de incidentes reportados, sesiones de capacitación realizadas, cumplimiento de copias de respaldo) con el fin de orientar acciones de mejora continua de manera realista.

13. Revisión y actualización

Esta política será revisada periódicamente o cuando se presenten cambios significativos en:

- El contexto organizacional (en la misión, estructura organizacional o procesos).
- La normatividad aplicable.
- Los riesgos de seguridad de la información.
- Los sistemas y tecnologías utilizadas por FENALCE.

14. Aprobación y adopción

La presente Política de Seguridad y Privacidad de la Información se adopta mediante resolución interna, y entra en vigor a partir de su aprobación y divulgación institucional.

Firma / Aprobación:

ARNULFO TRUJILLO DÍAZ
Gerente General

15. CONTROL DE CAMBIOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1.0	12/06/2026	Versión inicial

ELABORÓ	REVISÓ	APROBÓ
Nombre: Edna Espinosa Salazar	**Nombre:** Juan Ricardo Clavijo Silva	**Nombre:** Arnulfo Trujillo Díaz
CARGO: Jefe Oficina de Sistemas	**CARGO:** Jefe Oficina Jurídica	**CARGO:** Gerente General
Fecha: 30/Dic/2025	**Fecha:** 12/06/2026	**Fecha:** 12/06/2026