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 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES

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

1. Objetivo

Establecer los lineamientos institucionales para la identificación, reporte, registro, clasificación, análisis, contención, tratamiento, recuperación, comunicación, cierre y mejora continua frente a incidentes de seguridad de la información y, cuando aplique, de datos personales, con el fin de minimizar su impacto, preservar la continuidad de la operación, proteger los activos de información de FENALCE y fortalecer la resiliencia institucional.

2. Alcance

La presente Política es de obligatorio cumplimiento para FENALCE, sus dependencias, colaboradores, contratistas, proveedores, aliados estratégicos, encargados del tratamiento y terceros que, en virtud de su relación con la Federación, accedan, administren, procesen, custodien o usen información institucional o datos personales.

Aplica a:

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

- Todos los activos que soportan la información, incluyendo sistemas de información, infraestructura tecnológica, aplicaciones, redes, servicios en la nube, dispositivos, archivos físicos, bases de datos y repositorios documentales.

- Todos los eventos e incidentes que afecten o puedan afectar la confidencialidad, integridad o disponibilidad de la información, así como aquellos que comprometan datos personales.

Esta Política cubre tanto la gestión de incidentes de seguridad de la información como la atención de incidentes que involucren datos personales, en articulación con la Política Institucional de Seguridad y Privacidad de la Información, la Política Institucional de Tratamiento y Protección de Datos Personales y el Procedimiento de Gestión de Seguridad de la Información y Protección de Datos.

3. Marco de referencia y articulación institucional

La presente Política se adopta en concordancia con:

- Política de Seguridad y Privacidad de la Información de FENALCE.
- Política de Tratamiento y Protección de Datos Personales de FENALCE.
- Procedimiento de Gestión de Seguridad de la Información y Protección de Datos.
- Ley 1581 de 2012, el Decreto 1377 de 2013, el Decreto 1074 de 2015 y las directrices aplicables de la Superintendencia de Industria y Comercio.
- Buenas prácticas y lineamientos tomados como referencia por FENALCE en materia de seguridad de la información, incluyendo ISO/IEC 27001.

La presente Política desarrolla el componente de gestión de incidentes previsto en el marco institucional de seguridad y privacidad de la información de FENALCE y deberá interpretarse de manera sistemática con los demás documentos internos vigentes.

4. Definiciones

Para efectos de la presente Política, se adoptan las siguientes definiciones:

- **Activo de información:** Información, datos, documentos, sistemas, aplicaciones, infraestructuras tecnológicas, archivos físicos o digitales y demás elementos que tienen valor para FENALCE y requieren protección.
- **Evento de seguridad:** Situación observable, alerta, anomalía, debilidad, actividad sospechosa o falla detectada que puede derivar o no en un incidente de seguridad de la información. Esta definición se incorpora por criterio de gestión y control interno, en coherencia con el enfoque preventivo institucional.
- **Incidente de seguridad de la información:** Evento real o potencial que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información o de los datos personales tratados por FENALCE.
- **Incidente de datos personales:** Incidente de seguridad que afecta datos personales, incluyendo pérdida, acceso no autorizado, divulgación, alteración o destrucción indebida de los mismos.

- **Incidente crítico:** Incidente de alta severidad que afecta de manera significativa la operación, la continuidad de los servicios, el cumplimiento legal, la reputación institucional o la seguridad de datos personales o activos de información críticos. Esta categoría desarrolla la clasificación de severidad prevista en los documentos institucionales.

- **Contención:** Acciones inmediatas orientadas a limitar la propagación, alcance o impacto de un incidente.

- **Erradicación:** Acciones dirigidas a eliminar la causa técnica, lógica, física u organizacional del incidente.

- **Recuperación:** Restablecimiento seguro y controlado de los servicios, activos, procesos o datos afectados por el incidente.

- **Lecciones aprendidas:** Análisis posterior al incidente para identificar causas, debilidades, oportunidades de mejora y controles correctivos o preventivos.

5. Principios

La gestión de incidentes en FENALCE se regirá por los siguientes principios:

- **Reporte inmediato:** Toda persona vinculada a FENALCE deberá reportar inmediatamente cualquier incidente o sospecha que afecte o pueda afectar la seguridad y privacidad de la información.

- **Responsabilidad compartida:** La gestión de incidentes no es exclusiva de la Oficina de Sistemas; involucra a líderes de proceso, usuarios, contratistas, terceros, al Oficial de Seguridad de la Información y al Oficial de Protección de Datos Personales, según corresponda.

- **Trazabilidad y evidencia:** Todo incidente deberá quedar documentado de manera suficiente para soportar su análisis, tratamiento, cierre, seguimiento y eventual requerimiento de auditoría o autoridad competente.

- **Proporcionalidad y enfoque basado en riesgo:** La respuesta institucional será coherente con la severidad del incidente, el tipo de activo afectado, la sensibilidad de la información y los riesgos identificados.

- **Confidencialidad en la gestión:** La información relacionada con incidentes deberá ser conocida únicamente por las personas autorizadas,

preservando la reserva de evidencias, datos personales y elementos sensibles del caso.

- **Coordinación institucional:** La gestión de incidentes deberá articularse con los procesos jurídicos, tecnológicos, administrativos, contractuales y de comunicaciones cuando resulte necesario.

- **Mejora continua:** Todo incidente deberá aprovecharse como fuente de aprendizaje para fortalecer controles, capacidades, procedimientos y cultura organizacional.

- **Cultura de reporte sin represalias:** FENALCE promoverá el reporte oportuno y de buena fe de eventos e incidentes, evitando desincentivos injustificados para su comunicación.

6. Criterios de clasificación

Los incidentes deberán clasificarse, como mínimo, según su severidad, el tipo de información comprometida, el alcance del impacto, la criticidad del activo afectado y la necesidad de escalamiento interno o externo.

6.1. Clasificación por severidad

Nivel	Criterio general	Ejemplos orientadores	Tiempo de gestión inicial recomendado
Alto	Afectación crítica a la operación, activos estratégicos, información confidencial o datos personales; alto riesgo legal, reputacional o de continuidad.	Fuga de datos personales de productores, compromiso de credenciales privilegiadas, ransomware, indisponibilidad prolongada de sistemas críticos, acceso no autorizado a bases de datos institucionales.	Inmediato; priorización y escalamiento sin demora.
Medio	Afectación parcial o controlable, con impacto operativo moderado o riesgo acotado sobre información o servicios.	Caída de un sistema interno no crítico, envío indebido de información a un destinatario incorrecto sin exposición masiva,	Atención prioritaria durante la jornada o dentro del plazo definido por el

Nivel	Criterio general	Ejemplos orientadores	Tiempo de gestión inicial recomendado
		malware contenido oportunamente.	procedimiento interno.
Bajo	Eventos o incidentes menores, de impacto limitado, sin afectación significativa a la continuidad, la confidencialidad o el cumplimiento.	Intentos de phishing detectados sin compromiso efectivo, fallas menores corregidas localmente, eventos sospechosos sin impacto confirmado.	Registro, análisis y tratamiento conforme a capacidad operativa y criticidad.

Se considerarán críticos los incidentes que afecten información de productores, extensión agropecuaria o información estratégica de los subsectores de cereales, leguminosas y soya.

6.2. Criterios complementarios de clasificación

Adicionalmente, FENALCE podrá considerar, entre otros, los siguientes criterios para clasificar y priorizar incidentes:

- Tipo de activo de información afectado.
- Sensibilidad y clasificación de la información involucrada.
- Presencia de datos personales, especialmente sensibles o de menores de edad.
- Número de titulares o usuarios potencialmente afectados.
- Impacto sobre la operación gremial, administrativa, contractual, técnica, económica o de apoyo a la comercialización.
- Riesgo reputacional, contractual, financiero o legal.
- Necesidad de notificación a la Superintendencia de Industria y Comercio, a titulares o a terceros afectados.

7. Lineamientos para la gestión de incidentes

La gestión de incidentes en FENALCE sigue un ciclo estructurado de 8 etapas que van desde la identificación hasta la mejora continua, garantizando la respuesta coordinada en todos los niveles organizacionales, trazabilidad completa para auditoría y cumplimiento normativo, escalabilidad según severidad del incidente, articulación con las políticas marco de seguridad y privacidad de la información, así como aplicabilidad inmediata.

7.1. Identificación

Todo colaborador, contratista o tercero autorizado que detecte una situación anómala, una alerta, un incumplimiento de controles, un acceso no autorizado, una pérdida de información, una posible infección de malware, un error de configuración, una divulgación indebida o cualquier otra condición sospechosa deberá tratarla inicialmente como un evento de seguridad y reportarla de forma inmediata.

7.2. Reporte

El reporte de incidentes será obligatorio, inmediato y deberá realizarse a través de los canales institucionales definidos por FENALCE. Mientras dichos canales se formalizan o actualizan en el procedimiento operativo, deberán contemplar como mínimo la dirección de correo sistemas@fenalce.co, entre otros mecanismos internos que permitan dejar evidencia de la fecha, hora, reportante y descripción inicial del evento.

Deberán reportarse, entre otros, los siguientes casos:

- Pérdida, alteración, eliminación o indisponibilidad de información.
- Accesos no autorizados o sospechas de uso indebido de credenciales.
- Infecciones o sospechas de malware, ransomware o software malicioso.
- Envío erróneo, divulgación no autorizada o exposición indebida de información.
- Fallas de sistemas críticos, respaldos o mecanismos de recuperación.
- Cualquier incidente que comprometa datos personales.

7.3. Registro

Todo incidente reportado deberá registrarse en un expediente o bitácora centralizada de incidentes de seguridad de la información, y cuando involucre datos personales, también en el expediente correspondiente de incidentes de datos personales. El registro deberá permitir la trazabilidad del caso desde su detección hasta su cierre.

Como mínimo, el registro deberá incluir: fecha y hora de detección, fecha y hora de reporte, reportante, activo afectado, descripción del evento, clasificación preliminar, responsables de atención, acciones ejecutadas, decisiones de escalamiento, evidencias, impactos identificados, comunicaciones realizadas y fecha de cierre.

7.4. Análisis

Una vez reportado el incidente, el responsable designado de la Oficina de Sistemas deberá analizar su naturaleza, validar si corresponde a un evento o a

un incidente confirmado, determinar su severidad, identificar activos comprometidos, evaluar el alcance de la afectación y establecer si existe compromiso de datos personales, continuidad operativa o incumplimiento normativo.

Cuando el incidente involucre datos personales, el análisis deberá realizarse en articulación con el Oficial de Protección de Datos Personales, valorando el tipo de dato, el volumen de titulares afectados, la posible materialización de daños y la procedencia de notificaciones a la autoridad competente o a los titulares.

7.5. Respuesta

La respuesta al incidente deberá contemplar, según corresponda, acciones de contención, erradicación, recuperación y validación del restablecimiento del servicio o del control del riesgo. Estas acciones podrán incluir aislamiento de equipos, bloqueo o cambio de credenciales, suspensión temporal de accesos, activación de respaldos, restauración de servicios, corrección de configuraciones, aplicación de parches, retiro de archivos maliciosos y demás medidas técnicas, administrativas o físicas necesarias.

La recuperación deberá realizarse de manera controlada, verificando que el activo o servicio restablecido no mantenga la causa del incidente y que existan evidencias suficientes para soportar el cierre técnico y administrativo del caso.

7.6. Escalamiento y comunicación

FENALCE definirá en su procedimiento operativo las rutas de escalamiento según severidad, tipo de activo, impacto y naturaleza jurídica del incidente. Como criterio mínimo, los incidentes de severidad alta o aquellos que involucren datos personales, afectación reputacional, riesgo legal o interrupción relevante de servicios deberán escalarse de manera inmediata a la Gerencia General, al Oficial de Seguridad de la Información y, cuando corresponda, al Oficial de Protección de Datos Personales.

La comunicación del incidente deberá regirse por el principio de necesidad de conocer y por criterios de oportunidad, proporcionalidad, reserva y consistencia institucional. Ningún colaborador no autorizado podrá comunicar externamente incidentes en nombre de FENALCE.

Cuando el incidente comprometa datos personales, FENALCE evaluará y ejecutará, cuando aplique, la notificación a la Superintendencia de Industria y Comercio y a los titulares, de conformidad con la normativa vigente, la Política Institucional de Tratamiento y Protección de Datos Personales y el procedimiento interno correspondiente.

7.7. Cierre

El cierre del incidente solo procederá cuando se haya verificado, según corresponda: i) la contención del evento; ii) la erradicación o control razonable de la causa; iii) la recuperación del servicio o activo afectado; iv) la documentación suficiente del caso; v) la definición de acciones correctivas o preventivas; y vi) la consolidación de las lecciones aprendidas.

Los incidentes de alta severidad o aquellos que involucren datos personales deberán contar con una revisión de cierre validada por los responsables competentes en seguridad, tecnología y, cuando aplique, protección de datos personales.

7.8. Lecciones aprendidas y mejora continua

FENALCE realizará revisiones periódicas de incidentes y tendencias para identificar causas recurrentes, debilidades de control, necesidades de capacitación, ajustes en procedimientos, requerimientos tecnológicos y oportunidades de mejora. Los resultados deberán incorporarse, cuando corresponda, en los planes de mejora, en la gestión de riesgos, en la actualización de controles y en las actividades de sensibilización institucional.

8. Roles y responsabilidades

La gestión de incidentes de seguridad de la información y datos personales en FENALCE se desarrollará bajo el siguiente esquema general de responsabilidades:

Rol	Responsabilidades principales
Gerencia General	Apoyar la adopción de la política, tomar decisiones críticas ante incidentes de alto impacto, priorizar recursos y hacer seguimiento a los riesgos e incidentes relevantes.
Junta Directiva	Conocer la política, sus actualizaciones y, cuando corresponda, los reportes de riesgos, incidentes y planes de mejora.
Oficial de Seguridad de la Información (OSI)	Coordinar la implementación de la política, liderar o articular la gestión de incidentes, clasificar, escalar, hacer seguimiento, asegurar la documentación y promover acciones de mejora.
Profesionales de la Oficina de Sistemas	Administrar la infraestructura tecnológica, ejecutar y soportar controles técnicos, preservar evidencias técnicas, apoyar la contención, erradicación, recuperación, monitoreo y disponibilidad de servicios.

Oficial de Protección de Datos Personales (OPD)	Evaluar los incidentes que involucren datos personales, coordinar la atención jurídica y regulatoria, apoyar el análisis del impacto sobre titulares y gestionar, cuando aplique, las notificaciones ante la SIC y a los titulares.
Líderes de proceso y responsables de activos	Reportar incidentes, apoyar la valoración del impacto sobre sus procesos y activos, y asegurar la aplicación de medidas definidas.
Colaboradores, contratistas y terceros	Cumplir los lineamientos de seguridad, reportar de forma inmediata eventos o incidentes y colaborar con las acciones de respuesta cuando sean requeridos.

8.1. Criterio de implementación progresiva

Atendiendo la estructura y recursos de FENALCE, los roles de OSI y de atención operativa podrán implementarse de manera progresiva, siempre que exista una asignación expresa de responsabilidades y una adecuada articulación entre el/la Jefe de Sistemas y Oficial de Protección de Datos Personales. Este criterio resulta coherente con el enfoque institucional de proporcionalidad y con la realidad organizacional de la Federación.

9. Registros y evidencias

La gestión de incidentes deberá soportarse, como mínimo, en los siguientes registros institucionales, según corresponda:

- Registro y expediente de incidentes de seguridad de la información.
- Expediente de incidentes de datos personales.
- Comunicaciones de notificación a autoridad y titulares, cuando aplique.
- Registros de monitoreo, bitácoras técnicas, respaldos, restauraciones y evidencias asociadas.
- Informes de seguimiento, evaluación y planes de mejora derivados de incidentes.

Los registros deberán conservarse con criterios de integridad, disponibilidad, reserva y trazabilidad, conforme a las necesidades de auditoría, cumplimiento, defensa institucional y mejora continua.

10. Indicadores mínimos de seguimiento

Para fortalecer el seguimiento y la mejora continua, FENALCE podrá definir y monitorear indicadores básicos de gestión de incidentes, tales como: número de incidentes reportados por periodo, incidentes por severidad, tiempo de respuesta inicial, tiempo de cierre, incidentes con datos personales, incidentes recurrentes y porcentaje de acciones de mejora implementadas. Estos

indicadores son consistentes con el enfoque institucional de seguimiento realista y proporcional.

11. Incumplimiento

El incumplimiento de la presente Política podrá dar lugar a acciones administrativas, disciplinarias, contractuales o legales, según corresponda, sin perjuicio de las responsabilidades adicionales derivadas del manejo indebido de información, activos tecnológicos o datos personales.

12. Revisión, actualización y aprobación

La presente Política de Gestión de Incidentes se adopta mediante resolución interna, y entra en vigor a partir de su aprobación y divulgación institucional.

Firma / Aprobación:

ARNULFO TRUJILLO DÍAZ
Gerente General

13. 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