



*Nayarit*  
NUESTRA DIGNIDAD Y COMPROMISO

FONDOS DE FOMENTO  
INDUSTRIAL DE NAYARIT

Documento de Seguridad para la Protección de Datos Personales en Posesión del Fondo de Fomento Industrial del Estado de Nayarit, Órgano Administrador de los Fondos de Financiamiento del Gobierno del Estado de Nayarit, FIRCAES, FAEP y FOGAPET



- I. Presentación.
- II. Marco Normativo.
- III. Glosario.
- IV. Inventario de tratamientos de datos personales.
- V. Funciones y Obligaciones de las Personas que traten Datos Personales.
- VI. Análisis de Riesgo.
- VII. Análisis de Brecha.
- VIII. Plan de trabajo en materia de protección de datos personales.
- IX. Mecanismos de monitoreo y revisión de las Medidas de Seguridad.
- X. Programa de Capacitación.
- XI.** Actualización del Documento de Seguridad.



## I. Presentación

La ley de la materia establece que cada Sujeto Obligado deberá elaborar un Documento de Seguridad, en el que se establecerán las medidas de que se deberán adoptar, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee

En el mismo sentido este instrumento debe contar con el inventario de datos personales y de los sistemas de tratamiento, las funciones y obligaciones de los servidores que traten los datos personales, el análisis de riesgos, análisis de brecha, un plan de trabajo, mecanismos de monitoreo y revisión de las medidas de seguridad, así como un programa de capacitación en la materia.

El Documento de seguridad es un instrumento para conocer la situación actual, contemplando además de los datos personales en su poder, la vulnerabilidad a la que se encuentran, así como las acciones que van encaminadas a mejorar o reforzar la seguridad de los mismos.

Derivado de lo anterior, la Unidad de Transparencia de esta Entidad, dio inicio con los trabajos, de análisis de datos personales recabados por las distintas áreas que conforman esta Entidad, así como de los procesos a los que son sometidos y la finalidad de su captación.

En este documento se detallan las medidas de seguridad administrativas, físicas y técnicas con las que se contará en el Fondo de Fomento Industrial Órgano Administrador de los Fondos Estatales de Financiamiento, para garantizar la debida protección de los datos personales a los que se les da tratamiento en las Unidades Administrativas que los manejan. Dando así cumplimiento al artículo 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nayarit.



## II. Marco normativo

El presente instrumento se encuentra apegado a los que marcan los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos, al artículo 7, fracción XII Apartado B, de la Constitución Política del Estado Libre y soberano de Nayarit. Así como en la Ley de Transparencia y Acceso a la Información Pública del Estado de Nayarit, y lo establecido por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Nayarit.

## III. Glosario

Para los efectos de este Documento, además de las definiciones previstas en el artículo 4 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Nayarit, se entenderá por:

1. **Análisis de brecha:** Herramienta de análisis para comparar el estado y desempeño de las medidas de seguridad existentes de los sistemas de datos personales respecto de las faltantes, a partir de puntos de referencia seleccionados en una situación o momento dado.
2. **Análisis de riesgo:** Estudio de las posibles amenazas, vulnerabilidades y eventos no deseados que puedan producir afectaciones a los derechos patrimoniales o morales del titular de los datos personales.
3. **Comité:** Comité de Transparencia.
4. **Criterio:** Pauta que obliga a tomar en cuenta todos los elementos de un caso, disponibles para elegir de entre las posibles alternativas la mejor, con objeto de establecer los principios para la resolución de casos subsecuentes con la mayor certeza.
5. **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda



determinarse directa o indirectamente a través de cualquier información.

**6. Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones.

**7. Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

**8. Encargado:** Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

**9. FONAY:** Fondo de fomento Industrial del Estado de Nayarit, Órgano Administrador de los Fondos de Financiamiento del Gobierno del Estado de Nayarit, FIRCAES, FAEP y FOGAPET.

**10. Instituto o ITAI:** Instituto de Transparencia y Acceso a la Información Pública del Estado de Nayarit.

**11. Inventario de datos personales:** Catálogo de sistemas de datos con independencia de su forma de almacenamiento.

**12. LPDPPSOEN:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Nayarit

**13. Medidas de seguridad administrativas:** Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y



capacitación del personal, en materia de protección de datos personales.

**14. Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

**15. Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

**16. Portabilidad de datos personales:** Prerrogativa del titular de obtener una copia de los datos que ha proporcionado al responsable del tratamiento en un formato estructurado que le permita seguir utilizándolos.

**17. Políticas:** Definición de directrices estratégicas para la gestión y tratamiento de datos personales, alineadas a las atribuciones de la Institución. Incluye la elaboración y emisión interna de programas, entre otros documentos regulatorios.

**18. Titular:** Persona física a quien corresponden los datos personales.

**19. Responsable.** Responsable del Fondo a través de sus Unidades Administrativas.

**20. Servidor público vinculado:** El o los servidores públicos designados por los titulares de las Unidades Administrativas, encargados del tratamiento de datos personales.

**21. Sistema de Datos:** Archivo físico o electrónico que contenga datos personales que se hayan recabado para el ejercicio de las funciones de las Unidades Administrativas.

**22. Sistema de Gestión:** Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la Ley y las demás disposiciones que le resulten aplicables en la materia.



**23. Sistema Informático:** Conjunto de componentes de software interrelacionados, cuyo fin es el tratamiento de datos personales, mediante procedimientos automatizados.

**24. Unidad Administrativa:** Área a la que se le confieren atribuciones específicas en el Reglamento Interior, o en las Leyes aplicables.

**25. Unidad de Transparencia:** Instancia a la que hace referencia el artículo 124 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Nayarit.

**26. Documento de seguridad:** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

#### IV. Inventario y Catálogo de Datos Personales y de los Sistemas de Tratamiento.

En este apartado, se plasman los datos personales que las áreas administrativas obtienen a través de la documentación presentada, o el llenado de formatería de los titulares, para realizar los distintos procesos que se llevan a cabo en el Fondo de Fomento Industrial.

- 1. Datos de Identificación y contacto:** Nombre, estado civil, RFC, CURP, Numero de Seguridad Social, lugar de nacimientos, fecha de nacimientos, nacionalidad, domicilio, teléfono particular, teléfono celular, correo electrónico, firma autógrafa y referencias personales.
- 2. Datos empresariales:** Nombre de la microempresa, giro, dirección, tiempo de experiencia.
- 3. Datos Bancarios:** Cuentas Bancarias, pagos realizados, monto otorgado, y saldo.
- 4. Datos patrimoniales:** Bienes muebles e Inmuebles, Régimen Fiscal.
- 5. Datos legales:** Situación jurídica de la persona, sobre los juicios, amparos o procesos administrativos.

**Personas de quienes se obtienen los datos personales:**



*Nayarit*  
NUESTRA DIGNIDAD Y COMPROMISO

FONDOS DE FOMENTO  
INDUSTRIAL DE NAYARIT

- a. Personal que está en funciones en la Coordinación de Crédito.
- b. Personal que se encuentra en funciones en la Coordinación de Administración.
- c. Personal de la Coordinación Jurídica y de Cobranza.

Datos Personales en posesión de las Áreas Administrativas del FONAY

Área responsable del Sistema	Nombre del sistema	Datos personales recabados	Medio a través del cual se obtienen los datos	Finalidad del tratamiento	Tipo de datos	Servidores públicos que tienen acceso	Transferencia de datos	Nivel de seguridad
Dirección General	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica
Coordinación de Crédito	Solicitud de Créditos para emprendedores, y PYMES	Nombre, Dirección, Estado Civil, Edad, RFC, CURP, Teléfono, Correo electrónico. Datos de Empresa o actividad empresarial. Estado Civil, Régimen Fiscal, Datos Empresariales, Estado de Cuenta Datos patrimoniales (Garantías)	Físico	Análisis para saber si es candidato a otorgar un crédito.	Datos Personales	Coordinador de Crédito, y personal de la coordinación	No	Básico
Coordinación de Administración	Expediente para Recursos Humanos	Nombre, Dirección, Estado Civil, Edad, RFC, CURP, Numero de Seguridad Social, Teléfono, Correo electrónico	Físico	Integrar el Expediente de los Trabajadores	Datos Personales	Encargado de Departamento de Recursos Materiales y Capital Humano.	Si	Básico
Coordinación Jurídica y de Cobranza	Expedientes	Datos legales, expedientes de juicios mercantiles, administrativos, entre otros.	Físico	Integrar expedientes judiciales	Datos Personales	Personal de la Coordinación	Si	Básico
Coordinación de Archivos	Archivos	Nombre, Dirección, Estado Civil, Edad, RFC, CURP, Teléfono, Correo electrónico. Datos de Empresa o actividad empresarial. Estado Civil, Régimen Fiscal, Datos Empresariales, Estado de Cuenta Datos patrimoniales (Garantías)	Físico	Archivos	Datos Personales	Personal de la Coordinación	No aplica	Básico
Unidad de Transparencia	Solicitudes de Transparencia y Derechos ARCO, recibidos mediante la PNT	Nombre, Correo Electrónico	Electrónico / Físico	Solicitudes de Transparencia Derechos ARCO	Datos personales	Titular de la Unidad de Transparencia	Si	Básico



## Nivel de Seguridad de los datos personales a los que se les da tratamiento el en FONAY

A fin de garantizar la seguridad de los datos personales y en las bases de datos personales físicas y electrónicas, donde se encuentran los mencionados, las medidas de seguridad que se implementan corresponden a un nivel básico, protegiendo así la confidencialidad, integridad y disponibilidad de los datos personales tal como lo expresa la Ley de la materia

## Transferencias de datos personales

Toda transferencia de datos personales, se encontrara sujeta al consentimiento de su titular, salvo las excepciones previstas en la LPDPPSOEN.

## Catálogo de bases de datos personales de las Unidades Administrativas del FONAY

Cada Unidad Administrativa es la responsable del resguardo y tratamiento de los datos personales que maneja, esto con la finalidad de que el titular, conozca en donde se almacenan sus datos y más información relevante.

### V. Las funciones y obligaciones de las Personas que traten Datos Personales.

Las Unidades Administrativas encargadas de tratar datos personales son las siguientes

1. Dirección General
  - 1.1 Coordinación de Crédito
  - 1.2 Coordinación Jurídico y Cobranza
    - 1.2.1 Departamento de Jurídico
    - 1.2.2 Departamento de Cobranza
  - 1.3 Coordinación de Administración
    - 1.3.1 Departamento de Recursos Materiales y Humanos



- 1.4 Coordinación de Archivos
- 1.5 Unidad de Transparencia

Las personas que desempeñan los puestos anteriormente mencionados, tienen como funciones y obligaciones las siguientes:

1. Garantizar la seguridad en el tratamiento de datos personales, esto con la finalidad de evitar algún riesgo, tal como: pérdida, robo, alteración, publicación, distribución o acceso no autorizado.
2. Garantizar la debida protección de los datos personales, conforme a la Ley y a las demás disposiciones aplicables a la materia.
3. Implementar medidas de seguridad, tanto físicas, técnicas y administrativas, convenientes para el tratamiento diario de los datos personales.
4. Garantizar la confidencialidad de los datos personales derivado de los procedimientos que tiene a su cargo.
5. Conocer y aplicar las acciones derivadas de este Documento de Seguridad.
6. Garantizar el cumplimiento de los derechos ARCO a los titulares de los datos personales.

### **Registro de Incidencias.**

Las incidencias con datos personales que se produzcan, vulneraran la debida protección de estos, por lo tanto las Unidades Administrativas que traten con los mismos, deberán llevar un registro de aquellas incidencias que comprometan la seguridad de los datos en su poder.

Este registro deberá contener:

- a) Fecha del evento;



- b) Motivo;
- c) Acciones correctivas que se van a implementar de forma inmediata;
- d) Acciones definitivas;
- e) Nombre de la o el Responsable,
- f) Nombre de la o el Encargado;
- g) Cuando la vulneración se origine de un tratamiento de datos personales efectuado por el responsable;
- h) Causa de las vulneraciones;
- i) Persona quien registra;
- j) Persona a quien se informa; y
- k) Consecuencias.

El personal que trate datos personales, deberá contar con el registro de incidencias, ya que quien identifique la incidencia, será el encargado de registrar y notificar a su superior inmediato, quien a su vez se encargara de notificar a la o las personas afectadas para que este tome las precauciones debidas en caso de uso inadecuado de la información.

El responsable, deberá informar al titular lo siguiente:

- a) La naturaleza del incidente;
- b) Datos personales comprometidos;
- c) Recomendaciones al titular acerca de las medidas que se puedan adoptar para proteger sus intereses;
- d) Acciones correctivas realizadas de forma inmediata;
- e) Acciones legales para garantizar la recuperación de lo afectado; y
- f) La demás información que se establezca en las disposiciones jurídicas aplicables.

### **Sistema de administración y cartera de crédito.**

Actualmente el encargado de cobranza, es quien administra y asigna usuario y contraseña. La reserva, confidencialidad, y uso del sistema, queda bajo la responsabilidad de la persona a



quien se le asignó la cuenta de usuario. Por ningún motivo dichas cuentas pueden ser transferibles entre el personal.

En todo momento, las unidades administrativas que dan tratamiento a datos personales, deberán tener un control de acceso a sus bases de datos personales, deberán tener un control de acceso a su base de datos física o electrónica, en el cual establecerán las medidas de seguridad que salvaguarden la confidencialidad e integridad de la información resguardada.

Año tras año, las Unidades Administrativas, podrán enviar la información física que contenga datos personales a la Coordinación de Archivos del Fondo de Fomento Industrial.

## **VI. Análisis de Riesgo**

Se consideran como vulneraciones comunes las siguientes:

- a. La pérdida o destrucción no autorizada;
- b. El robo, extravió o copia no autorizada;
- c. El uso, acceso o tratamiento no autorizado;
- d. El daño, la alteración o modificación no autorizada, y
- e. Las demás previstas e las disposiciones jurídicas aplicables

## **VII. Análisis de Brecha.**

Una vez hecho un estudio con las unidades administrativas de sus medidas de seguridad, con la que tratan sus datos personales, se concluye que actualmente se tiene un nivel de medidas de seguridad bueno., mismas medidas que continuaran en mejora constante atendiendo a la optimización del manejo de datos personales.



## VIII. Plan de Trabajo en materia de protección de datos personales

El plan de trabajo para la protección de los datos personales que se llevara a cabo, contará con los siguientes pasos:

- a. Capacitar a los servidores públicos que dan tratamiento y tienen acceso a los datos personales.
- b. Implementar medidas de seguridad físicas, administrativas y técnicas para la debida protección de los datos personales.
- c. Llevar a cabo el seguimiento y verificación, con el fin de corroborar el cumplimiento de las obligaciones que marca la Ley.

## IX. Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad.

Las medidas de seguridad, administrativas, físicas y técnicas, serán de aplicación a todas las bases de datos personales que manejan las personas a cargo de las Unidades Administrativas del FONAY, de acuerdo a sus funciones y obligaciones

## X. Programa de Capacitación

La persona Titular de la unidad de Transparencia será el encargado de capacitar al personal del FONAY, en materia de protección de datos personales, al menos una vez al año, siendo el titular quien designe la fecha en la que se llevara a cabo la capacitación.

En caso de alguna modificación, actualización en la ley de la materia, se llevara aquella capacitación extraordinaria que satisfaga la necesidad de conocer las últimas modificaciones. Además cuando el Instituto, otorgue alguna capacitación, las áreas administrativas, tendrán que acudir a las mismas, a fin de



*Nayarit*  
NUESTRA DIGNIDAD Y COMPROMISO

FONDOS DE FOMENTO  
INDUSTRIAL DE NAYARIT

actualizarse y garantizar el óptimo tratamiento de los datos personales.

#### XI. Actualización del documento de seguridad.

El presente instrumento se actualizara cuando ocurran los siguientes casos:

1. Se produzcan modificaciones sustanciales al tratamiento de datos personales, que deriven en un cambio en el nivel de riesgo;
2. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema.
3. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad;
4. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad;
5. Cuando surja documentos formatos, recomendaciones, etc., por parte del ITAI para la mejora del documento de seguridad;
6. Por reformas a la LPDPPSOEN o a las disposiciones aplicables.



Registro de Incidencias	
Fecha de la incidencia:	Numero de Incidencia:
Motivo o Descripcion detallada de la incidencia	
Las acciones correctivas a implementar de forma inmediata y las definitivas	
Nombre y cargo de la persona que registra la incidencia	
Nombre y cargo de la persona a quien se le comunica la incidencia	
Causa de la incidencia	
Consecuencias de la incidencia	

\_\_\_\_\_  
Nombre y Firma de  
quien registra

\_\_\_\_\_  
Nombre y firma de  
enterado