PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES DEL FONDO DE CAPITALIZACIÓN E INVERSIÓN DEL SECTOR RURAL

ÍNDICE

1. INTRODUCCIÓN 3
2. GLOSARIO 3
3. OBJETIVO 6
4. MARCO JURÍDICO 8
5. RESPONSABLES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES. 9
6. APOYO E IMPULSO AL PROGRAMA 9
7. ALCANCE DEL PROGRAMA. 10
8. POLÍTICA DE GESTIÓN DE LOS DATOS PERSONALES 10
9. INVENTARIO DE BASE DE DATOS PERSONALES 10
10. CUMPLIMIENTO DE OBLIGACIONES 12
11. OBLIGACIONES RELEVANTES 13
12. FUNCIONES DEL COMITÉ DE TRANSPARENCIA 15
13. FUNCIONES DE LA UNIDAD DE TRANSPARENCIA 16
14. CAPACITACIÓN 17
15. SUPERVISIÓN Y AUDITORIAS 17
16. SANCIONES 18

1. INTRODUCCIÓN

Cabe señalar que la protección de los datos personales es un derecho reconocido en el sistema jurídico mexicano, de conformidad con lo establecido en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos, disposiciones que dieron la pauta para la promulgación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) instrumento normativo que fija los principios para el ejercicio efectivo del derecho fundamental de protección de datos personales en el sector público.

El Fondo de Capitalización e Inversión del Sector Rural (FOCIR) sujeto obligado y responsable en el tratamiento de datos personales que conforme a sus atribuciones lleve a cabo, garantizará la privacidad de todas las personas.

Por lo que, FOCIR, será el responsable del tratamiento de datos personales, y con la finalidad de cumplir con el principio de responsabilidad, está la elaboración de políticas y programas de protección de datos personales, obligatorios y exigibles al interior de este Fondo, por lo que, para la elaboración del presente Programa de Protección de Datos Personales, se identificaron las obligaciones que se deben cumplir y los principios que se deben observar en el tratamiento de datos personales, conforme a la etapa del ciclo de vida de los datos personales, lo anterior conforme a lo que establece la LGPDPPSO y demás normatividad que regula la materia, y a partir de ello, se definieron las acciones a seguir para su cumplimiento.

El presente Programa está basado en un sistema de gestión que permite proveer los elementos y actividades de dirección, operación y control de los procesos de FOCIR, para proteger de manera sistemática y continua los datos personales que estén en su posesión, entendiendo como un sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, así como, el cumplimiento de los principios, deberes y obligaciones previstos en dicha ley y las demás disposiciones que resulten aplicables en la materia.

2. GLOSARIO

Los términos que se utilizan en el presente Programa y que se relacionan a continuación, tendrán los significados siguientes, sea que se utilicen en su forma plural o singular, con o sin mayúscula:

Activo: Es cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, requipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización

Aviso de privacidad: Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Bases de datos: Conjunto ordenado de datos personales bajo criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.

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.

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.

Derechos ARCOP: Los derechos de acceso, rectificación, cancelación, oposición y portabilidad al tratamiento de datos personales.

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

Evaluación de impacto en la protección de datos personales: Evaluación mediante la cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

FOCIR: Fondo de Capitalización e Inversión del Sector Rural

Instituto o INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

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.

Programa: Programa de Protección de Datos Personales.

Responsable: Fondo de Capitalización e Inversión del Sector Rural al ser un sujeto obligado de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que decide sobre el tratamiento de los datos personales.

Revisión: Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este Programa.

Riesgo: Combinación de la probabilidad de un evento y su consecuencia desfavorable.

Sujeto obligado: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal.

Titular: Persona física a quien corresponden los datos personales.

Transferencias: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Unidad Administrativa: Unidad a la que se le confiere atribuciones específicas en el reglamento interior FOCIR.

Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

3. OBJETIVO

El Programa de Protección de Datos Personales tiene los siguientes objetivos:

1. Proveer las buenas prácticas en la protección de Datos Personales en posesión del Fondo de Capitalización e Inversión al Sector Rural.

2. Dar cabal cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales, así como la normatividad que derive de los mismos; y

3. Establecer mecanismos de Supervisión y vigilancia de las medidas de seguridad en Protección de Datos Personales.

Responsabilidades dentro del Programa.

En términos de los artículos 83 y 84, fracción I de la LGPDPPSO, que señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, por lo que este sujeto obligado tendrá las siguientes funciones:

I. Elaborar, aprobar, coordinar y supervisar el Programa, en conjunto con las unidades técnicas que estime necesario involucrar o consultar;

II. Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;

III. Dar a conocer el Programa al interior del sujeto obligado;

IV. Coordinar la implementación del Programa en las Unidades Administrativas del sujeto obligado;

V. Asesorar a las Unidades Administrativas en la implementación de este Programa.

VII. Supervisar la correcta implementación del Programa;

VIII. Elaborar, aprobar, coordinar y supervisar el programa anual de capacitación, en conjunto con las Unidades Administrativas que estime necesario involucrar o consultar, y

IX. Las demás que de manera expresa señale el propio Programa.

Para que los objetivos planteados se logren con éxito, el Programa requiere del apoyo e impulso directo del más alto nivel de FOCIR. En ese sentido, el Programa se deberá hacer del conocimiento de todas las Unidades Administrativas de FOCIR, a fin de que tome las medidas necesarias para su cabal cumplimiento.

La intervención de las Unidades Administrativas tendrá la finalidad única de impulsar la debida implementación del Programa al interior de este sujeto obligado, pero no podrá suplir ni afectar las funciones que otorgan los artículos 83 y 84 de la LGPDPPSO al Comité de Transparencia, en su carácter de máxima autoridad de datos personales en la organización.

Asimismo, para que la implementación del Programa tenga como resultado el cumplimiento integral de las obligaciones que establece la LGPDPPSO y los Lineamientos Generales, el Programa será de observancia obligatoria para todas las personas servidoras públicas de FOCIR que en el ejercicio de sus funciones traten datos personales.

Las Unidades Administrativas deberán realizar las acciones necesarias para cumplir con las obligaciones que establece este Programa, para lo cual deberán asignar los recursos materiales y humanos necesarios, y prever lo que se requiera en sus programas de trabajo.

Para ello, resulta fundamental que el Programa se conozca al interior de FOCIR, por lo que, el Comité de Transparencia se encargará de difundirlo entre las personas servidoras públicas.

En caso de que no se requiera el Oficial o no se cuente con los recursos para su designación, se valorará la posibilidad de designar a personal que asista a la Unidad de Transparencia o a la Dirección Jurídica en el cumplimiento de sus obligaciones en materia de protección de datos personales, el cual deberá contar con conocimientos técnicos sobre el derecho de protección de datos personales.

4. MARCO JURÍDICO

- Constitución Política de los Estado Unidos Mexicanos
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Lineamentos Generales de Protección de Datos Personales para el sector público.
- Procedimiento Interno para la Atención de Solicitudes de Ejercicio de Derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad.

- Mecanismos Internos de Supervisión y Vigilancia de las Medidas de Seguridad en Protección de Datos Personales.

5. RESPONSABLES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES.

El Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano tendrá las siguientes funciones con relación a este programa:

I. Elaborar, aprobar, coordinar y supervisar el Programa, en conjunto con las siguientes unidades:

- Titular de la Unidad de Administración y Finanzas.
- Titular de la Unidad de Promoción de Proyectos de Inversión.
- Titular de la Unidad de Operación y Programas Sectoriales.
- Titular de la Unidad de Seguimiento de Inversiones de Capital.

II. Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación.

III. Dar a conocer el Programa al interior de FOCIR.

IV. Coordinar la implementación del Programa en las Unidades Administrativas de FOCIR.

V. Asesorar a las Unidades Administrativas en la implementación de este Programa, con el apoyo de las unidades mencionadas en el numeral I.
VII. Supervisar la correcta implementación del Programa.

VIII. Elaborar, aprobar, coordinar y supervisar el programa anual de capacitación, en conjunto con las unidades técnicas que estime necesario involucrar o consultar.

6. APOYO E IMPULSO AL PROGRAMA

El Programa se deberá hacer del conocimiento del director general a fin de impulsar la debida implementación del Programa en todas las Unidades Administrativas.

7. ALCANCE DEL PROGRAMA.

El presente programa aplicará a todas las Unidades Administrativas que realicen tratamiento de datos personales en ejercicio de sus atribuciones, quienes además deberán de cumplir con los principios, deberes y obligaciones establecidas en la normatividad que regula la materia.

Quedan exceptuados de la aplicación de este programa, los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que refieren el artículo 120 de la Ley General de Transparencia y Acceso a la Información Pública y numeral 117 de la Ley Federal de Transparencia y Acceso a la Información Pública.

8. POLÍTICA DE GESTIÓN DE LOS DATOS PERSONALES

Se identificarán las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las Unidades Administrativas, de acuerdo con lo que establece la LGPDPPSO y según el ciclo de vida de los datos personales

OBTENCIÓN (Licitud, información, consentimiento, proporcionalidad, seguridad y confidencialidad).

USO Registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia, disposición. (Calidad, finalidad, lealtad, seguridad, confidencialidad)

ELIMINACIÓN (calidad y seguridad)

9. INVENTARIO DE BASE DE DATOS PERSONALES

Es necesario que cada una de las Unidades Administrativas realicen un diagnóstico de los tratamientos de datos personales que llevan a cabo, lo anterior, para la elaboración de un inventario de base de datos personales, el cual tendrá por lo menos los siguientes indicadores:

- Sujeto Obligado
- Unidad administrativa
- Tipo de archivo o base de datos
- Nombre del archivo o base de datos
- Fin y uso
- Fundamento legal de creación
- Nombre del administrador del archivo
- Nombre del encargado del archivo
- Número de personas servidoras públicas con acceso a la base de datos.
- Fecha de última actualización

En caso de transferir información de la base o sistemas que contengan datos personales, de forma total o parcial señale lo siguiente

- Tipo de transferencia
- Periodicidad de la transferencia
- Fundamento legal para realizar transmisión
- Finalidad de transmisión

Listar a quien o a quienes se le transfiere información de la base de datos distinta al titular de los datos (personas morales o físicas, otro sujeto obligado, etc.)

- Nombre de la persona

En caso de ser de tipo física (archivos en papel) especificar lo siguiente:

- Medio de resguardo
- Oficina en la que se resguarda
- Número de registros en la base de datos
- Medidas de seguridad

En caso de ser de tipo electrónica (sistemas informáticos, sonoros, magnéticos o audiovisuales)) especificar lo siguiente:

- Manejador o software utilizada para su administración de base de datos
- Sistema operativo en el cual está montada la base de datos
- Espacio físico en el cual se encuentra el equipo que almacena la Base de Datos

El diagnóstico en mención se basa en la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realizan en FOCIR.

Por "inventario de tratamientos de datos personales" se entenderá el control documentado que se llevará de los tratamientos que realizan las Unidades Administrativas del FOCIR, realizado con orden y precisión.

El inventario de datos personales al que hace referencia la LGPDPPSO en los artículos 33, fracción III, 35, fracción I, y 58 de los Lineamientos Generales, identificará los siguientes elementos relevantes:

10. CUMPLIMIENTO DE OBLIGACIONES

Se deberán observar las siguientes:

A. Obligaciones transversales. Los deberes de seguridad y confidencialidad deben observarse en cualquier etapa del ciclo de vida de los datos personales. Estas obligaciones se cumplen a través de los siguientes:

1. Documento de seguridad. Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad en Protección de Datos Personales, adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

2. Vulneraciones. Se considera como vulneración las siguientes:
- La pérdida o destrucción no autorizada;
- El robo, extravío o copia no autorizada;
- El uso, acceso o tratamiento no autorizado o
- El daño, la alteración o modificación no autorizada.

Cuando ocurra una vulneración el titular de la Unidad deberá notificar a la Unidad de Transparencia o al Encargado de Protección de Datos Personales, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud

de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

3. Principios. Se deberán observar los siguientes principios durante todas las etapas del ciclo del tratamiento de los datos personales, a saber:

a. Confidencialidad. Establecer controles o mecanismos para que todas las personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad, obligación que subsistirá aún después de finalizar sus relaciones con el mismo y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

b. Responsabilidad. Implementar las siguientes acciones para acreditar el cumplimiento de los principios, deberes y obligaciones, así como para rendir cuentas:
- Autorizar y destinar recursos para la instrumentación de programas y políticas de protección de datos personales.
- Elaborar el procedimiento interno para la atención de solicitudes en Derecho ARCOP.
- Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.
-Revisar periódicamente los mecanismos de Supervisión y Vigilancia a las medidas de seguridad en protección de Datos Personales, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.
- Establecer procedimientos para recibir y responder dudas y quejas de los titulares.
-Garantizar que las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la LGPDPPSO, los Lineamientos Generales y las demás que resulten aplicables en la materia.

11. OBLIGACIONES RELEVANTES

I. En la etapa de obtención de los datos personales, se deben observar los siguientes principios:

a. Licitud. Tratar los datos personales que posea sujetándose a las atribuciones o facultades de la normatividad aplicable.

b. Lealtad. Obtener los datos sin dolo, mala fe, engaño o negligencia.

c. Información. Poner a disposición del titular el aviso de privacidad al momento de la obtención de los datos personales. Difundir el aviso de privacidad por medios electrónicos y físicos. El aviso de privacidad deberá estar redactado conforme a la normatividad en materia de datos personales, para sus dos versiones integral y simplificado.

d. Consentimiento. Contar con el consentimiento del titular, para el tratamiento de sus datos personales, salvo que se actualice alguna de las excepciones previstas en el artículo 22 (excepciones para la obtención del consentimiento) de la LGPDPPSO. (Se debe considerar: Consentimiento menores de edad y personas en estado de interdicción o incapacidad declarada conforme a la Ley). Para este principio resulta importante resaltar que no se deben tratar datos personales sensibles salvo que se cuente con el consentimiento expreso del titular o se trate de los casos establecidos en el artículo 22 de la LGPDPPSO.

e. Proporcionalidad. Tratar los datos personales sólo cuando resulten adecuados, relevantes y necesarios para la finalidad que justifica su tratamiento. Se entenderá que los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención.

II. En la etapa de uso de los datos personales, se deben observar los siguientes principios:

a. Finalidad. Justificar el tratamiento de los datos personales en finalidades concretas, lícitas, explícitas y legítimas. Se entenderá que las finalidades son:
Concretas: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que

admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular.
Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.
Lícitas: cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades de la Unidad Administrativa que corresponda.
Legítimas: cuando las finalidades que motivan el tratamiento de los datos personales se encuentren habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General.

b. Calidad. Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales, principalmente cuando se obtuvieron de manera indirecta del titular. Se entenderá que los datos personales son:

Exactos y correctos: cuando los datos personales en posesión del responsable no presentan errores que pudieran afectar su veracidad.
Completos: cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable.
Actualizados: cuando los datos personales responden fielmente a la situación actual del titular.

III. En la etapa de eliminación de los datos personales, se deben observar los siguientes principios:

a. Supresión de datos personales. Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades y una vez que concluya su plazo de conservación establecido.

12. FUNCIONES DEL COMITÉ DE TRANSPARENCIA

El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales al interior del Fondo de Capitalización e Inversión del Sector Rural y al respecto, tendrá las siguientes funciones:

I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en FOCIR, de conformidad con las disposiciones previstas en la LGPDPPSO y en aquellas disposiciones que resulten aplicables en la materia;

II. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCOP;

III. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCOP;

IV. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la LGPDPPSO y en aquellas disposiciones que resulten aplicables en la materia;

V. Supervisar, en coordinación con las Unidades Administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en las medidas de seguridad;

VI. Dar seguimiento y cumplimiento a las resoluciones emitidas por el INAI;

VII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y

VIII. Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen las Unidades Administrativas.

13. FUNCIONES DE LA UNIDAD DE TRANSPARENCIA

La Unidad de Transparencia tendrá las siguientes funciones en materia de protección de datos personales:

I. Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales;

II. Gestionar las solicitudes para el ejercicio de los derechos ARCOP;

III. Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados;

IV. Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables;

V. Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCOP;

VI. Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCOP, y

VII. Asesorar a las Unidades Administrativas en materia de protección de datos personales.

14. CAPACITACIÓN

Establecer un programa anual de capacitación y actualización en materia de protección de datos personales, dirigido tanto a personal como a encargados.

El programa de capacitación deberá cubrir las necesidades dentro de la entidad y deberá ser aprobado por el Comité de Transparencia de FOCIR.

15. SUPERVISIÓN Y AUDITORIAS

Se deberá desarrollar o implementar los mecanismos de supervisión y vigilancia de las medidas de seguridad en protección de datos personales,

en términos del artículo 30, fracción V de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.

Dicho mecanismo contará con:

a) Mecanismo de monitoreo y supervisión.
b) Mecanismo de actuación ante vulneraciones a la seguridad de los datos personales
c) Mecanismo de auditoria en materia de datos personales.

Las revisiones administrativas las llevará a cabo el encargado de protección de datos personales, en caso de no contar con el encargado de protección de datos personales, la podrá realizar personal de adscrito a la Unidad de Transparencia

Asimismo, de conformidad con el artículo 151 de la LGPDPPSO, este sujeto obligado puede someterse voluntariamente a la realización de auditorías por parte del INAI.

16. SANCIONES

Cuando el Comité de Transparencia tenga conocimiento del incumplimiento de alguna obligación prevista en este Programa, deberá realizar, a la unidad administrativa correspondiente, un exhorto para que lleve a cabo las acciones que resulten pertinentes con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo que los pudieran ocasionar.

De manera adicional, es importante que los servidores públicos que están a cargo del tratamiento de datos personales tengan presente que de conformidad con el
artículo 163 de la LGPDPPSO serán causas de sanción por incumplimiento de las obligaciones establecidas en dicha ley, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCOP;

II. Incumplir los plazos de atención previstos en la LGPDPPSO para responder las solicitudes para el ejercicio de los derechos ARCOP o para hacer efectivo el derecho de que se trate;

III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la LGPDPPSO;

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la LGPDPPSO, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;

VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la LGPDPPSO;

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO;

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la LGPDPPSO;

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO;

XI. Obstruir los actos de verificación de la autoridad;

XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la LGPDPPSO;

XIII. No acatar las resoluciones emitidas por el Instituto, y

XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves.

Asimismo, de conformidad con el artículo 105 de los Lineamientos Generales, cuando alguna unidad administrativa se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCOP, ésta dará aviso al superior jerárquico para que le ordene realizar sin demora las acciones conducentes.

Si persiste la negativa de colaboración, la Unidad de Transparencia lo hará del conocimiento del Comité de Transparencia para que, a su vez, dé vista al órgano interno de control, dé inicio el procedimiento de responsabilidad administrativo respectivo.

Cabe destacar que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Las responsabilidades que resulten de los procedimientos administrativos correspondientes son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.