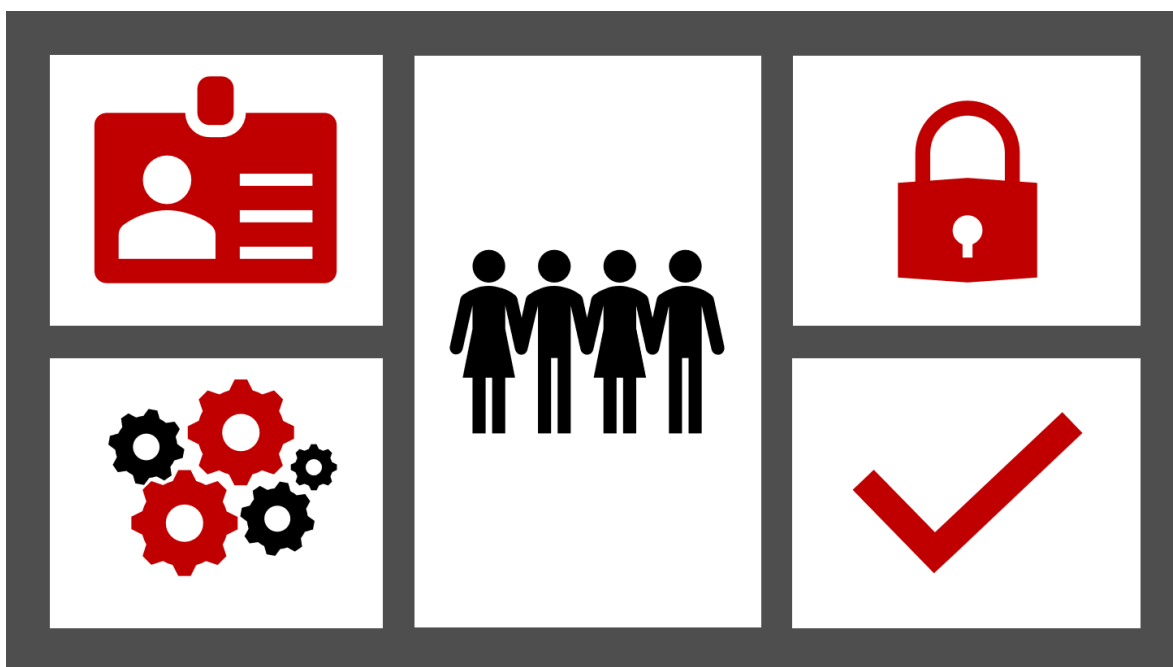


# Programa de Protección de Datos Personales del **INFONAVIT**



**Segunda edición**  
Septiembre 2024

**Programa de Protección de Datos Personales  
del Instituto del Fondo Nacional de la Vivienda para los Trabajadores  
(segunda edición)**

**Control de versiones**

<b>Versión</b>	<b>Descripción</b>	<b>Fecha</b>
Primera edición	Presentación y aprobación del Comité de Transparencia.	El 09 de febrero de 2022 en la sesión ordinaria 193.
Segunda edición	Presentación y aprobación del Comité de Transparencia.	El 09 de octubre de 2024 en la sesión ordinaria 225

## Contenido

<b>Glosario</b> .....	6
<b>Marco normativo</b> .....	9
<b>Preámbulo</b> .....	12
<b>Programa de Protección de Datos Personales 2ª edición</b> .....	15
<b>1. Objetivos</b> .....	15
<b>2. Alcance</b> .....	15
<b>3. Estrategias</b> .....	16
<b>Obligaciones en la etapa de obtención:</b> .....	17
<i>Licitud</i> .....	17
<i>Lealtad</i> .....	17
<i>Información</i> .....	18
<i>Medidas compensatorias</i> .....	19
<i>Consentimiento</i> .....	20
<i>Consentimiento de menores de edad y personas en estado de interdicción</i> .....	23
<i>Datos personales sensibles</i> .....	24
<i>Interés superior de los menores de edad</i> .....	24
<i>Proporcionalidad</i> .....	25
<b>Obligaciones en etapa de uso:</b> .....	25
<i>Finalidad</i> .....	25
<i>Calidad</i> .....	26
<i>Relación de encargados</i> .....	27
<i>Cómputo en la nube</i> .....	28
<i>Transferencias</i> .....	29
<i>Atención a solicitudes de ejercicio de derechos ARCOP</i> .....	31
<i>Trámite de atención</i> .....	32
<i>Requisitos de la solicitud de ejercicio de derechos ARCOP</i> .....	32
<i>Costos</i> .....	33
<i>Acreditación de la identidad</i> .....	34

<i>Acreditación de la identidad de menores de edad y personas en estado de interdicción o incapacidad conforme leyes civiles</i> .....	35
<i>Datos personales de persona fallecida</i> .....	35
<i>Requisitos generales de las respuestas</i> .....	36
<i>Cumplimiento del ejercicio de los derechos ARCOP</i> .....	37
<i>Modalidad de entrega</i> .....	39
<i>Incompetencia</i> .....	39
<i>Negativa</i> .....	40
<i>Trámite específico</i> .....	41
<i>Portabilidad</i> .....	41
<b>Obligaciones en la etapa de eliminación:</b> .....	41
<i>Supresión de los datos personales (calidad)</i> .....	41
<b>Obligaciones transversales:</b> .....	42
<i>Seguridad</i> .....	42
<i>Vulneraciones</i> .....	44
<i>Confidencialidad</i> .....	46
<b>Otras obligaciones:</b> .....	46
<i>Responsabilidad</i> .....	46
<i>Evaluación de impacto en la protección de datos personales</i> .....	48
<i>Funciones del Comité de Transparencia</i> .....	48
<i>Funciones de la Unidad de Transparencia</i> .....	49
<i>Capacitación</i> .....	51
<i>Revisiones y auditorias:</i> .....	51
<i>Acciones para la mejora continua</i> .....	52
<b>4. Roles y responsabilidades</b> .....	53
4.1 De la Alta Dirección .....	53
4.2 Del Comité de Transparencia .....	54
4.3 De las Unidades administrativas .....	54
4.4 De los Enlaces de transparencia y datos personales .....	54
4.5 De la Unidad de Transparencia .....	55
4.6 De la Oficial de Protección de Datos Personales .....	55

4.7 Del Oficial den Jefe de Seguridad de la Información .....	55
4.8 De las y los trabajadores del INFONAVIT .....	56
4.9 De los encargados.....	56
4.10 De la Subdirección General de Tecnologías de Información.....	56
<b>5. Causas de sanción.....</b>	<b>57</b>
<b>Asesoría y acompañamiento .....</b>	<b>58</b>

## Glosario

- **Análisis normativo:** Se trata de un formato a fin de primer acercamiento en el que la unidad administrativa realiza una identificación y análisis del tratamiento que reporta o del cual hace alguna consulta a la Unidad de Transparencia, a través, de la Oficial de Protección de Datos Personales, en el que manifiesta como da cumplimiento a las obligaciones en materia de datos personales, así como la contextualización del tratamiento que realiza o pretende
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva para determinar el grado de cumplimiento de los criterios preestablecidos para la misma.
- **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 referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
- **Cesi:** Centro de Servicio Infonavit
- **Comité de Transparencia o CT:** Autoridad máxima en materia de datos personales al interior del Infonavit, previsto en el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública, así como 83 y 84 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **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 mas 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 ARCO y Portabilidad:** Los derechos de acceso, rectificación, cancelación, oposición y portabilidad al tratamiento de datos personales.
- **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.

- **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. Comúnmente se les conoce como proveedores.
- **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.
- **INAI:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
- **Infonavit o Instituto:** Instituto del Fondo Nacional de la Vivienda para los Trabajadores.
- **Ley General de Datos o LGPDPSO:** 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.
- **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.
- **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.
- **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.
- **OPDP:** Oficial de Protección de Datos Personales.
- **OSI o CISO:** Oficial en Jefe de Seguridad de la Información.
- **Política:** Política de tratamiento y gestión de datos personales.
- **Portabilidad:** 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 del Infonavit.
- **Registro:** Registro de bases de datos con datos personales.

- **Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.
- **Responsable:** Infonavit
- **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.
- **SGTI:** Subdirección General de Tecnologías de Información.
- **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, así como el cumplimiento de los principios, deberes y obligaciones previstos en la Ley General de Datos y las demás disposiciones que resulten aplicables en la materia.
- **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:** áreas del Infonavit previstas en el Estatuto Orgánico, y normativa organizacional, que cuenta o puede contar, dar tratamiento, y ser responsables de datos personales.
- **Unidad de Transparencia o UT:** Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.



## Marco normativo

La **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados** prevé en sus artículos 29, 30, fracciones I y II, y 47 de los **Lineamientos Generales** el principio de responsabilidad y las acciones para cumplir con él, conforme lo siguiente:

**“Artículo 29. El responsable deberá implementar los mecanismos previstos en el artículo 30 de la presente Ley para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la presente Ley y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular e Instituto** o a los Organismos garantes, según corresponda, caso en el cual deberá observar la Constitución y los Tratados Internacionales en los que el Estado mexicano sea parte; en lo que no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines.”

**“Artículo 30. Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:**

- I. Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales;
- II. **Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable;**

[...]”

**“Políticas y programas de protección de datos personales**

**Artículo 47.** Con relación al artículo 30, fracciones I y II de la Ley General, **el responsable deberá elaborar e implementar políticas y programas de protección de datos personales** que tengan por objeto establecer los elementos y actividades de dirección, operación y control de todos sus procesos que, en el ejercicio de sus funciones y atribuciones, impliquen un tratamiento de datos personales a efecto de proteger éstos de manera sistemática y continua.

Las políticas y **programas de protección de datos personales** a que se refiere el párrafo anterior del presente artículo **deberán ser aprobados, coordinados y supervisados por su Comité de Transparencia.**

El responsable deberá prever y autorizar recursos, de conformidad con la normatividad que resulte aplicable, para la implementación y cumplimiento de éstos.”

[Énfasis añadido]

En ese contexto, el Programa de Protección de Datos Personales es la materialización de una de las obligaciones que suman al cumplimiento del principio de responsabilidad. El cual debe ser aprobado, coordinado y supervisado por el Comité de Transparencia.

También los artículos 83 y 84, de la **LGPDPPO** establecen lo siguiente:

**“Artículo 83. Cada responsable contará con un Comité de Transparencia, el cual se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.**

**El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales.”**

**“Artículo 84. Para los efectos de la presente Ley y sin perjuicio de otras atribuciones que le sean conferidas en la normatividad que le resulte aplicable, el Comité de Transparencia tendrá las siguientes funciones:**

- I. Coordinar, supervisar y **realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad**

con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;

[...]

- V. **Supervisar**, en coordinación con las áreas o unidades administrativas competentes, **el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;**

[...]"

**Artículo 85.** Cada responsable contará con una **Unidad de Transparencia**, se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública, esta Ley y demás normativa aplicable, que tendrá las siguientes funciones:

[...]

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

[...]

- 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 ARCO.**

[...]

Por su parte, el artículo 25 Bis 1 de la **Ley del Instituto del Fondo Nacional de la Vivienda para los Trabajadores** establece dentro de las funciones del Comité de Transparencia la de:

*"ARTICULO 25 Bis 1.- **Son funciones del Comité de Transparencia**, además de las establecidas en la Ley General y la Ley Federal en materia de Transparencia y Acceso a la Información Pública, las siguientes:*

[...]

III.- **Garantizar la protección de los datos personales en posesión del Instituto** y el ejercicio de los derechos de acceso, rectificación, corrección y oposición;

[...]

Asimismo, el **Manual de Organización de la Secretaría General y Jurídica**<sup>1</sup> establece de manera específica que la Gerencia Unidad de Transparencia tiene como uno de sus objetivos principales supervisar que el Infonavit cumpla con las disposiciones en materia de protección de datos personales, en apego a la Ley General de

Protección de Datos Personales en Posesión de Sujetos Obligados, con el objetivo de garantizar los derechos ARCO que realizan las y los titulares.

Para cumplir con lo anterior, una de sus principales funciones consiste en supervisar la implementación de los mecanismos para dar cumplimiento a los principios, deberes y obligaciones establecidos en la Ley General de Datos, como se muestra enseguida:

**"Funciones:**

- I. [...]

---

<sup>1</sup> Con clave de identificación MAN-INST-006, con fecha de elaboración 17 de diciembre de 2020, y fecha de publicación 11 de enero de 2021, versión 001.

- II. Supervisar la implementación de los mecanismos para dar cumplimiento a los principios, deberes y obligaciones establecidos en la LGPDPSO.

[...]

- VI. Supervisar el proceso de trámite de las solicitudes de información para garantizar el ejercicio de los derechos de Acceso a la Información y de los derechos ARCO; así como notificar a la Contraloría General el incumplimiento a la normativa aplicable.

[...]"

De la lectura de las disposiciones previas se advierte que, el Comité de Transparencia es la autoridad máxima en materia de datos personales, por ello tiene entre sus funciones la de realizar y supervisar las acciones necesarias para garantizar el derecho a la protección de datos personales en posesión del Instituto, entre ellas el Programa y demás acciones implementadas por el Infonavit para tratar los datos personales que manera segura y con apego a la normatividad de la materia.

Para ello, la Unidad de Transparencia tiene entre sus funciones la de 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 ARCO, así como establecer mecanismos para asegurar que los datos personales, solo se entreguen a su titular o representante.

## Preámbulo

El Infonavit ha realizado esfuerzos constantes en favor de la protección de los datos personales que trata, por lo que en seguimiento al **Programa** en su primera edición, realizó acciones conjuntas encabezadas por el Comité de Transparencia, operadas por la Unidad de Transparencia, la OPDP, el OSI y la Subdirección General de Tecnologías de la Información en colaboración con las unidades administrativas del Instituto con el propósito de que se cumplan las obligaciones en apego a la Ley General de Datos y su normativa derivada

La primera edición del Programa permitió mayor acercamiento con las unidades administrativas que presentaron interés en cumplir las obligaciones en datos personales. Lo anterior implicó requerir y revisar documentación, analizar las formas en que las unidades administrativas dan cumplimiento de las obligaciones de datos personales en los procesos implementados, así como en aquellos próximos a implementarse, ello permitió identificar áreas de oportunidad y en consecuencia en la suma de esfuerzos para continuar trabajando en las fortalezas y mejoras para el cumplimiento.

Esta nueva edición del Programa busca fortalecer los procedimientos diseñados en su primera edición para garantizar el derecho a la protección de datos personales de las personas titulares de los datos que posee el Instituto; además, pretende hacer frente a las amenazas a la privacidad e intimidad identificadas como uno de los problemas a nivel nacional e internacional y sus posibles consecuencias en otros derechos fundamentales.

Continuar con el apego y mejora del Programa lo consolidará como un marco completo y actualizable que permita dar seguimiento y guía respecto de las acciones para proteger los datos personales en el Instituto.

En este apartado se presenta un resumen de las actividades más relevantes durante febrero de 2022 a septiembre de 2024, periodo que abarcó el Programa en su primera versión.

### 2022

- Diseño e implementación del curso *Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*.
- Atención de investigaciones previas y procedimientos de verificación ante el INAI.
- Capacitaciones específicas a personal de los Cesi sobre datos biométricos.
- Elaboración del *Protocolo de atención a denuncias de posibles casos de usurpación de identidad*.
- Aprobación de la **Política de Tratamiento y Gestión de Datos Personales** por el Comité de Transparencia en su sesión ordinaria número 194 de fecha 9 de

marzo de 2022, y posteriormente por la Asamblea General del Instituto el 28 de abril de 2022, entrando en vigor el 29 de abril de 2022.

- Elaboración y publicación de avisos de privacidad, principalmente el de la PBI.
- Se elaboró y presentó la primera *Evaluación de Impacto en la Protección de datos Personales* ante el INAI. Lo anterior, derivado de la implementación de la Plataforma Biométrica Institucional (PBI), de conformidad con lo dispuesto en los artículos 74 y 75 de la Ley General de Datos, así como las *Disposiciones de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales*.
- Participación en el Grupo de Trabajo de la Plataforma Biométrica Institucional (PBI).
- Rediseño del Apartado virtual "Protección de Datos Personales".
- Atención de consultas técnicas para el cumplimiento de principios y deberes.

## 2023

- Seguimiento a la realización, por parte del personal del Instituto, de los dos cursos sobre protección de datos personales en Universidad Infonavit. *Derecho a la protección de datos personales e Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, con más del 50% de participación del personal, es decir, una plantilla de más de 4,500 trabajadores y trabajadoras.
- Cumplimiento a resolución de procedimiento de verificación.
- Difusión mediante Webmaster de las Políticas de tratamiento y gestión de datos personales.
- Participación en el *Grupo de Gobierno de Datos* con derecho a voz y voto.
- Participación en el *Grupo de Seguridad de la Información* con derecho a voz y voto.
- Comienzo de las acciones transversales para cumplir con el *Plan de Implementación de Recomendaciones no vinculantes (PIR)* de la PBI.
- Desarrollo de la actualización de los *Lineamientos de Transparencia, Acceso a la Información, Archivos y Protección de Datos Personales del Instituto del Fondo Nacional de la Vivienda para los Trabajadores*, los cuales contemplan el reconocimiento de los Enlaces de transparencia y datos personales, así como la obligación de constante capacitación en la materia.
- Elaboración de avisos de privacidad.
- Atención de consultas técnicas para el cumplimiento de principios y deberes.

## 2024

- Cursos en Universidad Infonavit sobre protección de datos personales, con 94% de participación del personal en el denominado *Derecho a la protección de datos personales* y un 90% del curso llamado *Introducción a*

la LGPDPPSO, considerando que el total de la plantilla laboral es de 5,919 personas.

- Realización de acciones para cumplir con el PIR, respecto de la Evaluación de Impacto en la Protección de Datos Personales de la PBI.
- Publicación de los **Lineamientos de Transparencia, Acceso a la Información, y Protección de Datos Personales del Instituto del Fondo Nacional de la Vivienda para los Trabajadores**, desarrollando temas y figuras de protección de datos personales.
- Elaboración y actualización de avisos de privacidad.
- Capacitación específica a personal de los Cesi y de la Unidad de Transparencia en *Lengua de Señas Mexicana* para dar una atención incluyente a personas que acudan a solicitar el ejercicio de derechos ARCO y de Portabilidad y que tengan una discapacidad auditiva.
- Atención de investigaciones previas y procedimientos de verificación.
- Participación en reuniones de trabajo multidisciplinarias, entre las unidades administrativas, el Grupo de Gobierno de Datos y la OPDP para el análisis de la sensibilidad de datos personales.
- Participación en la *Estrategia de Gobierno de Datos*.
- Acompañamiento en la *Campaña de actualización del expediente laboral*, en colaboración de la Subdirección General de Administración y Recursos Humanos.
- Elaboración de la *Metodología específica para el análisis de riesgos en materia de datos biométricos – huellas dactilares-*.
- Colaboración con la Subdirección General de Operaciones para lograr la *Certificación a nivel clase mundial en el Modelo Global de Calidad para la Interacción con Clientes (MGCIC) versión 3.0*, respecto a su apartado 7.1. *Sistema de Gestión de seguridad de la información y datos personales (SGSDP)*.
- Como resultado de la primera Verificación vinculante en materia de protección de datos personales, realizada por el INAI el Instituto obtuvo 85% de cumplimiento de un total de 100%.
- Atención de consultas técnicas para el cumplimiento de principios y deberes.

## Programa de Protección de Datos Personales 2ª edición

### 1. Objetivos

Para esta segunda edición se tiene como **objetivo principal** la mejora en los mecanismos para acreditar el cumplimiento de las obligaciones derivadas de los principios, deberes y derechos, conforme a lo establecido en la Ley General de Datos, a través de tres estrategias.

- Estrategia para el cumplimiento de los principios de protección de datos personales.
- Estrategia para el fortalecimiento de la cultura en protección de datos personales (eje transversal).
- Estrategia para el cumplimiento de los deberes de seguridad y confidencialidad.

Para lograr lo anterior, se continuará con acciones para:

- Fortalecer la cultura por la protección de datos personales.
- Promocionar el marco de trabajo necesario para la protección de los datos personales en posesión del Infonavit.
- Revisar los análisis normativos e inventarios de datos personales a fin de alinear aquellos que presenten áreas de oportunidad.
- Establecer los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua.
- Identificar mejores prácticas en la protección de datos personales, que puedan ser implementadas de manera integral en el Instituto, o bien, cuando se estime pertinente en tratamientos específicos.
- Capacitar a personal en temas de protección de datos personales.
- Mejorar el Sistema de Gestión de seguridad en datos personales a fin de fortalecerlo.

### 2. Alcance

El Programa para esta edición aumentó su alcance ya que además de las actividades del personal de todas las unidades administrativas y Órganos Colegiados, en esta oportunidad también se sumaron los esfuerzos de la Dirección Sectorial de Trabajadores, la Dirección Sectorial Empresarial, Auditoría Interna, así como el Comité Ejecutivo Nacional, que realizan tratamientos de datos personales en el ejercicio de sus funciones.



### 3. Estrategias

Para que el Instituto cumpla con los objetivos señalados, la Unidad de Transparencia y la OPDP determinaron continuar con el desarrollo de tres estrategias:

**a) Estrategia para el cumplimiento de los principios de protección de datos personales.**

**Objetivo:** Revisar que las unidades administrativas del INFONAVIT, que tratan datos personales como parte de sus funciones, cumplan con los principios (licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad e información) que rigen la protección de los datos personales, establecidos en la Ley General de Datos, demás normativa aplicable y los mecanismos establecidos.

**b) Estrategia para el fortalecimiento de la cultura en protección de datos personales (eje transversal).**

**Objetivo:** Fortalecer la cultura de la protección de datos personales entre el personal del Instituto para garantizar el cumplimiento de las obligaciones en la materia, a través de acciones de sensibilización y campañas de difusión.

**c) Estrategia para el cumplimiento de los deberes de seguridad y confidencialidad.**

**Objetivo:** Fortalecer a nivel institucional el cumplimiento de los deberes de seguridad y confidencialidad establecidos en la Ley General de Datos y demás disposiciones aplicables para la salvaguarda de los datos personales.

Las estrategias para cumplimiento de principios y fortalecimiento de la cultura de protección de datos personales serán desarrolladas por la Unidad de Transparencia a tres años (2024-2027), mientras que la vinculada a los deberes de seguridad y confidencialidad serán conforme lo determine el OSI.

#### **Estrategia para el cumplimiento de los principios de protección de datos personales**

A continuación, se identifican las obligaciones que establecen la Ley General de Datos y los Lineamientos Generales y se dividen según las distintas etapas del ciclo de vida de los datos personales (obtención, uso y eliminación), señalando la siguiente información:

- Descripción de las obligaciones.
- Actividades a realizar para su cumplimiento.
- Evidencia

Para todos los tratamientos de datos personales se debe cumplir con todos los principios y deberes que establecen la LGPDPSO, los Lineamientos Generales y



demás normatividad que resulte aplicable, en cualquier momento del tratamiento o ciclo de vida de los datos personales.

El desglose de las obligaciones, conforme el ciclo de vida es:

- Obtención
- Uso
- Eliminación
- Transversales
- Otras obligaciones

### Obligaciones en la etapa de obtención:

#### Licitud

Obligaciones	Actividades para su cumplimiento	Evidencia
Sujetar el tratamiento de los datos personales a las atribuciones o facultades que la normatividad aplicable confiera al Infonavit, así como con estricto apego y cumplimiento de lo dispuesto en dicho ordenamiento, los Lineamientos Generales, la legislación mexicana que le resulte aplicable y, en su caso, el derecho internacional, respetando los derechos y libertades de los titulares.	Identificar el marco normativo (leyes, tratados o acuerdos internacionales, reglamentos, lineamientos, entre otros, con sus respectivos artículos) que faculta a la unidad administrativa a tratar los datos personales para cada una de las finalidades, y aquél que regula el tratamiento respectivo.	<ul style="list-style-type: none"> <li>• Marco normativo respectivo interno y externo.</li> <li>• Análisis normativo</li> </ul>

#### Lealtad

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>• No obtener ni tratar los datos personales a través de medios engañosos o fraudulentos.</li> </ul> <p>De acuerdo con el artículo 11, fracción I, de los Lineamientos Generales, se entiende por medios engañosos y fraudulentos aquéllos que se utilicen para tratar los datos personales con dolo, mala fe o negligencia.</p>	1. Verificar que los datos personales no se obtengan con dolo, mala fe o negligencia.	<ul style="list-style-type: none"> <li>• Medios para la obtención de los datos personales.</li> <li>• Resultado de las auditorías o procedimientos de revisión efectuados.</li> </ul>
<ul style="list-style-type: none"> <li>• Privilegiar los intereses y expectativa razonable de privacidad de los titulares.</li> </ul> <p>De acuerdo con el artículo 11, fracción II de los Lineamientos Generales, se entenderá que el Infonavit privilegia los intereses del titular cuando el tratamiento de datos personales no da lugar a discriminación o trato injusto o arbitrario en contra del titular.</p>	<p>2. Verificar los tratamientos que realiza el Infonavit, a fin de confirmar que los mismos no den lugar a discriminación o trato injusto o arbitrario en contra del titular.</p> <p>3. Elaborar avisos de privacidad con todos los elementos informativos que establece la LGPDPSO, y con información que corresponda a la realidad del tratamiento que se efectúa.</p>	<ul style="list-style-type: none"> <li>• Avisos de privacidad.</li> <li>• Documentación que se genere durante el tratamiento, que permita acreditar que los datos personales se utilizaron conforme a lo señalado en el</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
<p>Asimismo, de conformidad con el artículo 11, fracción III de los Lineamientos Generales, se entiende por expectativa razonable de privacidad, la confianza que el titular ha depositado en el Infonavit respecto a que sus datos personales serán tratados conforme a lo señalado en el aviso de privacidad y en cumplimiento a las disposiciones previstas en la LGPDPSO y los Lineamientos Generales.</p> <p>Esta obligación deberá observarse a lo largo de todo el ciclo de vida de los datos personales, desde la obtención de los mismos hasta su eliminación.</p>	<p>4. Incluir en los avisos de privacidad todas las finalidades de los tratamientos, las cuales deberán estar redactadas de forma clara y concreta, para que no haya lugar a confusión al respecto.</p> <p>5. Llevar a cabo el tratamiento de los datos personales sólo para los fines informados en el aviso de privacidad.</p>	<p>aviso de privacidad, y según lo dispuesto en la normatividad.</p> <ul style="list-style-type: none"> <li>• Resultado de las auditorías o procedimientos de revisión efectuados.</li> </ul>

## Información

Obligaciones	Actividades para su cumplimiento	Evidencia
<p>Informar a los titulares las características principales del tratamiento al que serán sometidos sus datos personales, a través del aviso de privacidad.</p>	<p>1. Poner a disposición de las personas titulares el aviso de privacidad.</p>	<p>Fotografías de lugares o identificación de los medios en los que se colocan los avisos de privacidad.</p>
<p>Contar con los avisos de privacidad necesarios.</p>	<p>2. Redactar los avisos de privacidad que se requieran conforme a los tratamientos que lleven a cabo las unidades administrativas.</p> <p>Como regla general, se requerirá un aviso de privacidad <b>por tratamiento</b>.</p> <p>Sólo en los casos en que la información a incluir en el aviso de privacidad de distintos tratamientos sea la misma en su mayoría, se podrá redactar un aviso de privacidad común. El criterio para este supuesto es que la redacción del aviso de privacidad compartido no sea confusa.</p>	<p>Avisos de privacidad</p>
<p>Cumplir con las características en la elaboración del aviso de privacidad.</p>	<p>3. Redactar los avisos de privacidad con claridad, sencillez, información necesaria, comprensible, atendiendo al perfil del titular a quien va dirigido</p>	<p>Avisos de privacidad</p>
<p>Contar con los avisos de privacidad en sus dos modalidades con todos los elementos necesarios.</p>	<p>4. Redactar las dos modalidades para cada aviso de privacidad: simplificado e integral.</p>	<p>Avisos de privacidad</p>
<p>Implementar mecanismos para que el titular pueda manifestar su negativa para el tratamiento de datos personales para finalidades o transferencias que requieran el consentimiento,</p>	<p>5. Diseñar mecanismos que permitan al titular manifestar su negativa previa al tratamiento o transferencia de sus datos personales, cuando se requiera su consentimiento para ello.</p>	<p>Avisos de privacidad</p>

Obligaciones	Actividades para su cumplimiento	Evidencia
previo a que ocurra el tratamiento.		
<ul style="list-style-type: none"> <li>Difundir el aviso de privacidad por medios electrónicos, físicos, ópticos, sonoros, visuales o por cualquier otra tecnología.</li> <li>Ubicar el aviso de privacidad en un lugar visible que facilite la consulta del titular y que le permita acreditar fehacientemente el cumplimiento de esta obligación ante el INAI.</li> </ul>	<p>6. Poner a disposición todos los avisos de privacidad, en sus modalidades simplificada e integral, en el portal de Internet de la institución, en la sección que se destine para ello, a fin de que se difunda por medios electrónicos.</p> <p>De manera adicional, los avisos de privacidad deberán estar disponibles para su consulta en medio impreso (físico) en las instalaciones de la institución, en donde resulte conveniente según el medio por el que se obtengan los datos personales y por el que se tenga contacto con los titulares.</p> <p>Asimismo, cuando ello sea necesario o conveniente, el aviso de privacidad se podrá dar a conocer por otros formatos y medios, como por ejemplo en formato sonoro, vía telefónica, entre otros.</p> <p>6. Ubicar los avisos de privacidad en lugares visibles, que faciliten su consulta por parte del titular, tomando en cuenta su formato (físico, electrónico, óptico, sonoro, visual o de la tecnología de que se trate) y el medio por el que se dé a conocer.</p>	<ul style="list-style-type: none"> <li>Fotografías de los lugares o identificación de los medios en los que se difundieron y colocaron los avisos de privacidad.</li> <li>Documentación para poner en producción del portal institucional el aviso de privacidad correspondiente.</li> <li>Portal institucional, apartado de protección de datos personales</li> </ul>
<p>Observar los momentos para la puesta a disposición:</p> <ul style="list-style-type: none"> <li>De manera previa a la obtención de los datos personales, cuando los mismos se obtengan directamente del titular, sin importar el formato y medio, o</li> <li>Al primer contacto con el titular o previo al aprovechamiento de los datos personales, cuando éstos se obtengan de manera indirecta del titular.</li> </ul>	<p>7. Implementar mecanismos para dar a conocer el aviso de privacidad en los momentos antes señalados, según sea el caso.</p>	<p>Procedimientos para puesta a disposición de los avisos de privacidad, en los procesos o especificaciones técnicas</p>

### Medidas compensatorias

Obligaciones	Actividades para su cumplimiento	Evidencia
<p>Instrumentar medidas compensatorias cuando resulte imposible dar a conocer al titular el aviso de privacidad simplificado de manera directa, o ello exija esfuerzos desproporcionados, de acuerdo con los Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal.</p>	<p>1. Dar a conocer el aviso de privacidad simplificado a través de la implementación de medidas compensatorias cuando: i) resulte imposible dar a conocer al titular el aviso de privacidad de manera directa, o ii) ello exija esfuerzos desproporcionados.</p> <p>2. Evaluar si se requiere o no la autorización expresa del INAI para la implementación de medidas compensatorias, según lo dispuesto por los Criterios Generales para la</p>	<p>Evidencia de la difusión del aviso de privacidad por el medio de comunicación masiva utilizado para la medida compensatoria implementada.</p>

Obligaciones	Actividades para su cumplimiento	Evidencia
	<p>instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal.</p> <p>3. Implementar las medidas compensatorias de conformidad con lo dispuesto por los Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal.</p>	<p>En su caso, autorización del INAI y evidencia de su difusión.</p>

## Consentimiento

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>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 de la LGPDPSO, que señala lo siguiente:                     <p><b>Artículo 22.</b> El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:</p> <p><b>I.</b> Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla;</p> <p><b>II.</b> Cuando las transferencias que se realicen entre responsables sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;</p> <p><b>III.</b> Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;</p> <p><b>IV.</b> Para el reconocimiento o defensa de derechos del titular ante autoridad competente;</p> <p><b>V.</b> Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;</p> <p><b>VI.</b> Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;</p> <p><b>VII.</b> Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;</p> <p><b>VIII.</b> Cuando los datos personales figuren en fuentes de acceso público;</p> <p><b>IX.</b> Cuando los datos personales se sometan a un procedimiento previo de disociación, o</p> <p><b>X.</b> Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.</p> <p>La actualización de alguno de los supuestos anteriores no exime al responsable del cumplimiento de las demás</p> </li> </ul>	<ol style="list-style-type: none"> <li>Identificar las finalidades para las cuales se requiere el consentimiento de los titulares.</li> <li>En esos casos, solicitar el consentimiento de los titulares según las reglas.</li> </ol>	<ul style="list-style-type: none"> <li>Consentimiento expreso otorgado por los titulares y la solicitud respectiva.</li> <li>Aviso de privacidad, en su caso.</li> <li>Justificación de que aplica alguna de las excepciones a la obtención del consentimiento, la cual podrá estar prevista en el análisis normativo o de manera específica.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
obligaciones establecidas en la LGPDPPSO y los Lineamientos Generales.		
<ul style="list-style-type: none"> <li>El consentimiento que, en su caso, se obtenga debe ser <b>libre, específico e informado</b>, según lo dispuesto por el artículo 20 de la LGPDPPSO.</li> <li>Por otra parte, la solicitud del consentimiento deberá ser concisa e inteligible, estar redactada en un lenguaje claro y sencillo acorde con el perfil del titular y, cuando se refiera a diversos asuntos ajenos a la protección de datos personales, deberá presentarse de tal forma que se distinga claramente de dichos asuntos.</li> </ul>	<p>3. Solicitar el consentimiento después de que se ponga a disposición del titular el aviso de privacidad.</p> <p>4. Redactar las solicitudes de consentimiento de forma tal que éste sea libre, específico e informado, y que las solicitudes sean concisas e inteligibles, estén en un lenguaje claro y sencillo acorde con el perfil del titular, y se distingan de asuntos ajenos a la protección de datos personales, cuando ello sea necesario.</p>	<ul style="list-style-type: none"> <li>Procedimiento implementado para la solicitud del consentimiento.</li> <li>Procedimiento para la puesta a disposición del aviso de privacidad.</li> <li>Texto de solicitud de consentimiento.</li> </ul>
<ul style="list-style-type: none"> <li>Dependiendo del tipo de datos personales, el consentimiento deberá ser tácito o expreso, siguiendo las reglas establecidas en el artículo 21 de la LGPDPPP: <ul style="list-style-type: none"> <li>Quando los datos sean sensibles y no se actualice alguna de las causales del artículo 22 de la LGPDPPSO, se requerirá el consentimiento <b>expreso y por escrito</b>, es decir, a través de la firma autógrafa o firma electrónica del titular, o por medio del mecanismo de autenticación que para tal efecto se establezca.</li> <li>El consentimiento <b>expreso</b> se solicitará cuando así lo exija una ley o las disposiciones aplicables.</li> <li>En todos los demás casos se podrá obtener el consentimiento <b>tácito</b>.</li> </ul> </li> </ul> <p>El consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en contrario.</p> <p>El consentimiento será expreso cuando la voluntad del titular se manifieste de forma verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.</p> <p>Se entenderá que:</p> <ul style="list-style-type: none"> <li>El titular <b>otorga su consentimiento de manera verbal</b> cuando lo externe oralmente de manera presencial o mediante el uso de cualquier otra tecnología que permita la interlocución oral, en ambos casos, ante la persona que represente al Infonavit, y</li> </ul>	<p>5. Definir el tipo de consentimiento que se requiere, según las categorías de datos personales que se vayan a tratar o las disposiciones normativas que regulen el tratamiento.</p> <p>6. Habilitar los mecanismos necesarios para solicitar el consentimiento expreso, en los términos señalados en la columna anterior, así como documentar su obtención.</p> <p>7. Documentar la puesta a disposición del aviso de privacidad para la obtención del consentimiento tácito.</p>	<ul style="list-style-type: none"> <li>Solicitud del consentimiento expreso.</li> <li>Consentimiento expreso otorgado por los titulares.</li> <li>Puesta a disposición del aviso de privacidad.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>El titular <b>otorga su consentimiento por escrito</b> cuando manifieste su voluntad en un documento, físico o electrónico, a través de cierta declaración en sentido afirmativo, firma autógrafa, huella dactilar, firma electrónica o cualquier mecanismo o procedimiento equivalente autorizado por la normatividad aplicable.</li> </ul> <p>La carga de la prueba para acreditar la obtención del consentimiento expreso correrá a cargo del Infonavit.</p>		
<ul style="list-style-type: none"> <li>Cuando los datos personales se recaben <b>directamente</b> del titular, y se requiera al consentimiento, éste deberá solicitarse previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad.</li> </ul> <p>Se entenderá que el responsable obtiene los datos personales directamente del titular cuando es éste quien los proporciona o la persona que lo representa, personalmente o por algún medio que permita su entrega directa como podrían ser medios electrónicos, ópticos, sonoros, visuales, vía telefónica, Internet o cualquier otra tecnología y/o medio.</p>	<p>8. Solicitar el consentimiento previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad, cuando los datos personales se obtengan directamente de su titular o representante.</p>	<ul style="list-style-type: none"> <li>Procedimiento para la solicitud del consentimiento.</li> <li>Aviso de privacidad y procedimiento para su puesta a disposición.</li> <li>Consentimiento expreso otorgado.</li> </ul>
<ul style="list-style-type: none"> <li>Cuando los datos personales se obtengan <b>indirectamente</b> del titular, y se requiera el consentimiento, no se podrán tratar los datos personales hasta que se cuente con la manifestación libre, específica e informada del titular, en la que autorice el tratamiento de sus datos personales de manera tácita o expresa, según corresponda.</li> <li>De conformidad con el segundo y tercer párrafo del artículo 15 de los Lineamientos Generales, el titular tendrá un plazo de cinco días, contados a partir del día siguiente de recibir el aviso de privacidad por parte del responsable, para que, en su caso, manifieste su negativa al tratamiento de sus datos personales a través de los medios establecidos por el responsable.</li> </ul> <p>En caso de que el titular no manifieste su negativa en el plazo antes señalado, se entenderá que ha otorgado su consentimiento tácito para el tratamiento de sus datos personales, salvo prueba en contrario.</p> <p>Se entenderá que se obtienen los datos personales de manera indirecta cuando no se cumplan con las condiciones señaladas en el apartado anterior.</p>	<p>9. Cuando los datos personales no los proporcione personal o directamente el titular o su representante, el Infonavit deberá enviar a los titulares el aviso de privacidad correspondiente al medio de contacto que tenga registrado. Asimismo, deberá informarles que cuentan con un plazo de 5 días hábiles para en su caso manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que requieran su consentimiento.</p> <p>Si el titular no manifiesta su negativa en el plazo de cinco días antes señalado, el Infonavit podrá suponer que cuenta con el consentimiento tácito.</p> <p>En el caso del consentimiento expreso, es necesario que el mismo se solicite, ya sea en el cuerpo del aviso</p>	<ul style="list-style-type: none"> <li>Aviso de privacidad.</li> <li>Constancia de envío del aviso de privacidad.</li> <li>Respuesta por parte de los titulares.</li> <li>Consentimiento expreso otorgado.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
	de privacidad o en un instrumento aparte. El Infonavit no podrá tratar los datos personales si no cuenta con el consentimiento expreso del titular.	
<ul style="list-style-type: none"> <li>Atender las solicitudes de revocación del consentimiento, mismas que podrán ser presentadas por el titular en cualquier momento del tratamiento sin que se le atribuyan efectos retroactivos, a través del ejercicio de los derechos de oposición y cancelación.</li> </ul>	<p>10. Prever en el procedimiento interno para la atención de solicitudes de derechos ARCO lo relativo a la revocación del consentimiento, según los plazos, requisitos y procedimiento que se establecen para el ejercicio de los derechos de cancelación y oposición.</p>	<ul style="list-style-type: none"> <li>Procedimiento interno atención derechos ARCO.</li> </ul>

### Consentimiento de menores de edad y personas en estado de interdicción

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Atender las reglas de representación previstas en el Código Civil Federal y demás disposiciones que resulten aplicables en la materia específica de que se trate, para la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley.</li> </ul> <p>Asimismo, tomar como referencia lo dispuesto en los artículos 78 a 81 de los Lineamientos Generales para acreditar la identidad de los menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley.</p>	<ol style="list-style-type: none"> <li>Identificar los tratamientos de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, que requieren consentimiento, según el artículo 22 de la LGPDPSO.</li> <li>Poner a disposición de los padres, tutores o representantes legales el aviso de privacidad, así como también, cuando ello sea posible, a los menores de edad y al titular en estado de interdicción o incapacidad declarada conforme a ley.</li> <li>Redactar los avisos de privacidad y solicitudes de consentimiento en lenguaje sencillo, adaptado para la comprensión del menor de edad o de la persona que se encuentre en estado de interdicción o incapacidad declarada conforme a ley.</li> <li>Implementar mecanismos que permitan tener certeza que quien otorga el consentimiento, está facultado legalmente para ello, máxime cuando el mismo no se vaya a requerir con la presencia física de los padres, tutores o representantes legales.</li> </ol> <p>Se sugiere consultar estos mecanismos previamente con el Comité de Transparencia y/o el OPDP.</p>	<ul style="list-style-type: none"> <li>Documentación que acompañe la solicitud y el otorgamiento del consentimiento por parte de los padres, tutores o representantes legales.</li> </ul>



### Datos personales sensibles

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>No 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.</li> </ul>	<ol style="list-style-type: none"> <li>Revisar la necesidad y legalidad del tratamiento de datos personales sensibles para cumplir con la finalidad de que se trate, a fin de que quede debidamente justificada su obtención y uso.</li> <li>Revisar que se actualice alguno de los supuestos del artículo 22 de la LGPDPPSO, o bien, en caso contrario, solicitar el consentimiento expreso y por escrito del titular.</li> </ol>	<ul style="list-style-type: none"> <li>Marco normativo que habilita para el tratamiento de datos personales sensibles.</li> <li>Consentimiento del titular, en su caso, o la actualización de alguno de los supuestos previstos en el artículo 22 de la LGPDPPSO.</li> </ul>
<ul style="list-style-type: none"> <li>No llevar a cabo tratamiento de datos personales que tengan como efecto la discriminación de los titulares por su origen étnico o racial, su estado de salud presente, pasado o futuro, su información genética, sus opiniones políticas, su religión o creencias filosóficas o morales y su preferencia sexual.</li> </ul>	<ol style="list-style-type: none"> <li>Verificar que el tratamiento de datos personales no tenga como consecuencia discriminación de los titulares.</li> </ol>	<ul style="list-style-type: none"> <li>Documentación que se genere en torno al tratamiento.</li> </ul>

### Interés superior de los menores de edad

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Privilegiar el interés superior del niño, niña y adolescente en el tratamiento de sus datos personales, en términos de las disposiciones previstas en la Ley General de los Derechos de Niñas, Niños y Adolescentes, así como lo dispuesto en la Ley General y los Lineamientos Generales.</li> </ul>	<ol style="list-style-type: none"> <li>En todos los casos en que estén involucrados datos personales de menores de edad, tener siempre en cuenta y privilegiar el interés superior del menor de edad.</li> <li>Conocer la Ley General de Niñas, Niños y Adolescentes, con objeto de conocer los derechos de los menores de edad y las obligaciones al respecto.</li> <li>Poner a disposición el aviso de privacidad tanto al adulto que tenga la representación del menor, como al propio titular de los datos personales.</li> <li>Solicitar el consentimiento del adulto que tenga la representación del menor, cuando éste se requiera, y de manera adicional solicitar la opinión del propio titular.</li> </ol>	<ul style="list-style-type: none"> <li>Documentación o procedimiento que acredite la puesta a disposición del aviso de privacidad al adulto que tenga la representación del menor de edad y al propio titular de los datos personales.</li> <li>Documento que acredite la obtención del consentimiento del adulto que tiene la representación del menor, así como la opinión del propio titular.</li> <li>Capacitación o curso realizado en materia de la Ley General de Niñas, Niños y Adolescentes, o bien, difusión de la misma.</li> </ul>



## Proporcionalidad

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Tratar los datos personales sólo cuando resulten adecuados, relevantes y necesarios para la finalidad que justifica su tratamiento.</li> </ul>	<ol style="list-style-type: none"> <li>Identificar qué datos personales se requieren para cada una de las finalidades. El listado de datos personales debe estar completo con independencia de que en el aviso de privacidad se informe por categoría de datos.</li> <li>Analizar y revisar que se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate.</li> <li>Cuando una normativa establezca con precisión los datos personales que deberán obtenerse para cumplir con la finalidad de que se trate, sólo deberán solicitarse dichos datos.</li> </ol>	<ul style="list-style-type: none"> <li>Avisos de privacidad.</li> <li>Documentos, expedientes, archivos o bases de datos correspondientes al tratamiento.</li> <li>Normatividad que establezca, en su caso, los datos personales que deberán solicitarse para el tratamiento específico.</li> <li>Análisis normativo</li> </ul>
<ul style="list-style-type: none"> <li>Realizar esfuerzos razonables para limitar los datos personales tratados, al mínimo necesario, con relación a las finalidades que motivaron su tratamiento.</li> </ul>	<ol style="list-style-type: none"> <li>Requerir el mínimo posible de datos personales para lograr las finalidades para las cuales se tratan.</li> </ol>	

## Obligaciones en etapa de uso:

### Finalidad

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Justificar el tratamiento de los datos personales en finalidades concretas, lícitas, explícitas y legítimas.</li> </ul>	<ol style="list-style-type: none"> <li>Identificar las finalidades de cada tratamiento que se realice, y verificar que las mismas atiendan a fines específicos o determinados, y que sean acordes a las atribuciones o facultades del Infonavit y unidad administrativa de que se trate.</li> <li>Verificar que en los avisos de privacidad se informan todas las finalidades para las cuales se tratan los datos personales, y que éstas se describen de manera clara.</li> <li>Identificar qué finalidades requieren consentimiento y solicitarlo según las reglas descritas anteriormente.</li> </ol>	<ul style="list-style-type: none"> <li>Avisos de privacidad.</li> <li>Inventario de tratamientos de datos personales.</li> <li>Documentos que se generen en el tratamiento.</li> <li>Análisis normativo</li> </ul>
<ul style="list-style-type: none"> <li>Las finalidades deben estar relacionadas con las atribuciones normativas de la unidad administrativa que realice el tratamiento.</li> </ul>	<ol style="list-style-type: none"> <li>Identificar el marco normativo (ley, reglamento, lineamiento, entre otros, con sus respectivos artículos) que otorga las atribuciones a la unidad administrativa para tratar los datos personales para cada una de las finalidades.</li> </ol>	<ul style="list-style-type: none"> <li>Marco normativo.</li> </ul>
<ul style="list-style-type: none"> <li>Cuando se vayan a tratar los datos personales para finalidades distintas a las previstas en el aviso de privacidad, se requiere tener atribuciones legales para ello y el consentimiento del titular,</li> </ul>	<ol style="list-style-type: none"> <li>Identificar las finalidades que no fueron informadas en los avisos de privacidad y que se requieran llevar a cabo.</li> <li>Verificar que existan atribuciones legales para el tratamiento de los datos personales para estas finalidades adicionales.</li> </ol>	<ul style="list-style-type: none"> <li>Marco normativo.</li> <li>Consentimiento otorgado por los titulares o supuesto que se actualiza del artículo 22 de la LGPDPSO.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
<p>salvo que se trate de una persona desaparecida.</p> <p>Se deberá considerar:</p> <ol style="list-style-type: none"> <li>I. La expectativa razonable de privacidad del titular, basada en la relación que tiene con éste;</li> <li>II. La naturaleza de los datos personales;</li> <li>III. Las consecuencias del tratamiento posterior de los datos personales para el titular, y</li> <li>IV. Las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la Ley General y los presentes Lineamientos generales.</li> </ol>	<p>7. Solicitar el consentimiento de los titulares para el tratamiento de datos personales para estas finalidades adicionales, cuando el mismo se requiera.</p> <p>8. Implementar las medidas que se requieran para cumplir con las obligaciones que establece la LGPDPPSO y los Lineamientos Generales, con relación a las finalidades adicionales.</p>	

### Calidad

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>• Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales, principalmente cuando se obtuvieron de manera indirecta del titular.</li> </ul>	<p>1. Implementar medidas para que los datos personales se actualicen y, en su caso, corrijan o completen, en las distintas bases de datos que estén a cargo de la unidad administrativa.</p> <p>Estas medidas deberán permitir que la modificación de los datos personales sea inmediata, una vez que la unidad administrativa tenga conocimiento de la actualización o corrección a que haya lugar.</p>	<ul style="list-style-type: none"> <li>• Base de datos actualizada y correcta.</li> <li>• Constancias o anotaciones sobre la rectificación realizada, en aquellos casos en que la misma haya sido precedente.</li> <li>• Análisis normativo</li> </ul>
<ul style="list-style-type: none"> <li>• Establecer plazos de conservación de los datos personales, los cuales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, asimismo deberán atender las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.</li> </ul>	<p>2. Establecer los plazos de conservación de los datos personales, para cada uno de los tratamientos, lo cual deberá ser congruente con los plazos de conservación establecidos en los instrumentos de clasificación archivística.</p>	<ul style="list-style-type: none"> <li>• Instrumentos de clasificación archivística.</li> </ul>
<ul style="list-style-type: none"> <li>• Establecer y documentar los procedimientos para la conservación y supresión de los datos personales, en los cuales se incluyan los periodos de conservación, mecanismos que permitan cumplir con</li> </ul>	<p>3. Elaborar los procedimientos para la conservación y supresión de los datos personales, así como documentarlos.</p> <p>Estos procedimientos podrán ser los establecidos en materia de archivos, si a</p>	<ul style="list-style-type: none"> <li>• Procedimientos desarrollados.</li> <li>• Documentación y evidencia que se genere con su implementación.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
dichos plazos, así como realizar una revisión periódica sobre la necesidad de conservar los datos personales.	través de los mismos se puede cumplir con la obligación prevista en la LGPDPPSO.	

### Relación de encargados

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Formalizar las relaciones con los encargados mediante contrato o instrumento jurídico, que permita acreditar su existencia, alcance y contenido.</li> </ul> <p>Incluir en el contrato o instrumento jurídico, al menos, lo previsto en los artículos 59 y 61 de la LGPDPPSO y 108 a 110 de los Lineamientos Generales.</p>	<p>1. Formalizar las relaciones con los encargados mediante contrato o instrumento jurídico, que contenga las obligaciones y cláusulas antes señaladas.</p>	<ul style="list-style-type: none"> <li>Cláusulas tipo</li> <li>Contratos o instrumentos jurídicos.</li> <li>Registro de encargados.</li> </ul>
<ul style="list-style-type: none"> <li>Autorizar las subcontrataciones que realicen los encargados y que involucren el tratamiento de datos personales.</li> <li>Informar al encargado que el contrato o el instrumento jurídico mediante el cual se formalice la subcontratación deberá incluir cláusulas con las obligaciones antes señaladas.</li> </ul>	<p>2. Incluir en los contratos originales con los encargados una cláusula que haga referencia a lo que procederá en caso de que el encargado desee subcontratar servicios que involucren el tratamiento de datos personales.</p> <p>En el contrato original se podrá autorizar o prohibir de manera directa la subcontratación de este tipo de servicios, o bien, se podrá establecer que para la subcontratación será necesario que el encargado solicite autorización expresa al responsable, caso por caso.</p> <p>Las autorizaciones se podrán otorgar desde el contrato original, cuando el encargado ya prevea subcontrataciones específicas, y garantice que las mismas se realizarán en las condiciones antes señaladas. En caso contrario, la autorización se realizará de manera posterior. Para el cumplimiento de esta obligación, es necesario que el contrato o el instrumento jurídico, celebrado de origen con el encargado, establezca que las subcontrataciones que no se establezcan de manera expresa en dicho contrato o instrumento deberán ser autorizadas por el responsable.</p> <p>Asimismo, si se van a autorizar las subcontrataciones o quedará abierta dicha posibilidad, será necesario que en el contrato original entre el responsable y el encargado, se establezca que si este último pretende llevar a cabo subcontrataciones deberá suscribir un contrato o instrumento jurídico con el tercero de que se trate, en el que se</p>	<ul style="list-style-type: none"> <li>Cláusula tipo</li> <li>Contratos o instrumentos jurídicos.</li> <li>Registro de encargados.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
	deberán prever las cláusulas a las que refiere la columna anterior como parte de las obligaciones del subcontratado.	

### Cómputo en la nube

Obligaciones	Actividades para su cumplimiento	Evidencia
<p>Contratar servicios de cómputo en la nube y similares con proveedores que garanticen políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la LGPDPPSO, los Lineamientos Generales y demás disposiciones que resulten aplicables en la materia.</p> <p>Delimitar el tratamiento de datos personales a través de cláusulas contractuales u otros instrumentos jurídicos.</p>	<p>1. Verificar las cláusulas contractuales antes de la contratación, con objeto de garantizar que el servicio cumpla con los requisitos que establece la LGPDPPSO.</p>	<ul style="list-style-type: none"> <li>• Contratos o instrumentos jurídicos.</li> <li>• Registro de encargados</li> </ul>
<p>Contratar sólo servicios de cómputo en la nube que cumplan, al menos, con lo siguiente:</p> <ul style="list-style-type: none"> <li>o Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la LGPDPPSO y demás normativa aplicable;</li> <li>o Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;</li> <li>o Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y</li> <li>o Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.</li> </ul>	<p>2. Sólo contratar servicios de cómputo en la nube que garanticen los requisitos antes señalados.</p> <p>En caso de que los contratos se hayan celebrado antes de la entrada en vigor de la LGPDPPSO, será necesario que para su modificación o renovación, en caso de que ello fuera a ocurrir, se revise que los mismos cumplen con las condiciones antes señaladas, pues de lo contrario no podrán renovarse ni modificarse en los mismos términos.</p>	
<p>Contratar sólo servicios de cómputo en la nube que cuenten con mecanismos, al menos, para:</p> <ul style="list-style-type: none"> <li>o Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;</li> <li>o Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;</li> <li>o Establecer y mantener medidas de seguridad para</li> </ul>	<p>3. Sólo contratar servicios de cómputo en la nube que garanticen los requisitos antes señalados.</p> <p>En caso de que los contratos se hayan celebrado antes de la entrada en vigor de la LGPDPPSO, será necesario que, para su modificación o renovación, se revise que los mismos cumplen con las condiciones antes señaladas, pues de lo contrario no podrán renovarse ni modificarse en los mismos términos.</p>	

Obligaciones	Actividades para su cumplimiento	Evidencia
<p>la protección de los datos personales sobre los que se preste el servicio;</p> <ul style="list-style-type: none"> <li>o Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos, e</li> <li>o Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, está obligado a informar de ese hecho al responsable.</li> </ul>		
<p>No contratar o adherirse a servicios que no garanticen la debida protección de los datos personales, conforme a la LGPDPPSO y demás disposiciones que resulten aplicables en la materia.</p>	<p>(No hay actividades designadas, al ser una prohibición y no un mandato de hacer).</p>	
<p>Cuando el responsable tenga la posibilidad de convenir con el proveedor las condiciones y términos del servicio, además de observar las obligaciones antes señaladas -específicas para servicios de cómputo en la nube-, se deberá incluir en el contrato o instrumento jurídico las obligaciones generales de cualquier encargado.</p>	<p>4. En su caso, incluir en el contrato o instrumento jurídico que formalice la contratación de los servicios, las obligaciones generales de cualquier encargado.</p>	<ul style="list-style-type: none"> <li>• Contratos o instrumentos jurídicos.</li> </ul>

### Transferencias

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>• Formalizar las transferencias nacionales e internacionales mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes, salvo en las siguientes excepciones: <ul style="list-style-type: none"> <li>o Cuando la transferencia sea nacional y se realice entre el Infonavit y otros responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos, o</li> <li>o Cuando la transferencia sea internacional y se encuentre prevista</li> </ul> </li> </ul>	<ol style="list-style-type: none"> <li>1. Identificar las transferencias que se realizan que requieren la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.</li> <li>2. Elaborar y suscribir las cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, cuando se requiera.</li> </ol>	<p>Documento que demuestre el detalle operativo y/o funcional de la comunicación.</p>

Obligaciones	Actividades para su cumplimiento	Evidencia
<p>en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el Infonavit y el responsable receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento que realiza el Infonavit.</p>		
<ul style="list-style-type: none"> <li>Sólo hacer transferencias fuera del territorio nacional cuando el tercero receptor se obligue a proteger los datos personales conforme a los principios y deberes que establece la LGPDPPSO y las disposiciones que resulten aplicables en la materia.</li> </ul>	<p>3. Para las transferencias y remisiones internacionales, previo a que éstas ocurran, se deberá solicitar al tercero receptor que <u>manifieste por escrito</u> que se obliga a proteger los datos personales conforme a los principios y deberes que establece la LGPDPPSO y las disposiciones que resulten aplicables en la materia.</p>	<ul style="list-style-type: none"> <li>Escritos de los terceros receptores de los datos personales.</li> </ul>
<ul style="list-style-type: none"> <li>Comunicar el aviso de privacidad respectivo al tercero receptor en las transferencias nacionales e internacionales que se realicen.</li> </ul>	<p>4. Cuando inicien las transferencias, comunicar el aviso de privacidad correspondiente.</p> <p>En lo sucesivo, sólo comunicar las modificaciones al aviso de privacidad original, cuando existan.</p>	<ul style="list-style-type: none"> <li>Evidencia de la comunicación del aviso de privacidad.</li> <li>Documento que demuestre el detalle operativo y/o funcional de la comunicación.</li> </ul>
<p>Solicitar el consentimiento para las transferencias nacionales e internacionales, salvo excepciones.</p>	<p>5. Identificar las transferencias que requieren consentimiento de los titulares e informarlo en el aviso de privacidad.</p> <p>6. Solicitar el consentimiento de los titulares previo a la transferencia, cuando éste sea necesario y según la modalidad que se requiera (tácito o expreso y por escrito).</p>	<ul style="list-style-type: none"> <li>Consentimiento de los titulares.</li> </ul>
<ul style="list-style-type: none"> <li>En caso de que se requiera el consentimiento expreso, establecer el medio que permita obtenerlo de manera previa a la transferencia.</li> </ul>	<p>7. Establecer los medios para solicitar el consentimiento expreso, previo a la transferencia.</p>	<ul style="list-style-type: none"> <li>Medios establecidos para solicitar el consentimiento expreso, en caso de requerirse.</li> </ul>
<ul style="list-style-type: none"> <li>Sólo tratar los datos que hayan sido transferidos al responsable para las finalidades para las cuales le hayan sido comunicados, según lo establecido en el aviso de privacidad proporcionado, así como garantizar la confidencialidad de los datos personales.</li> </ul>	<p>8. Implementar los controles de seguridad establecidos para la confidencialidad de los datos personales, y no tratar los datos personales para finalidades distintas.</p>	<ul style="list-style-type: none"> <li>Documento que demuestre el detalle operativo y/o funcional de la comunicación.</li> </ul>

## Atención a solicitudes de ejercicio de derechos ARCO

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO.</li> </ul> <p>El procedimiento respectivo deberá considerar la obligación del personal de orientar, en su caso, a los titulares sobre la localización de la Unidad de Transparencia.</p> <p>El Infonavit podrá establecer los plazos y los procedimientos internos que considere convenientes para recibir, gestionar y dar respuesta a las solicitudes para el ejercicio de los derechos ARCO, observando, en todo momento, los requisitos, condiciones, plazos y términos previstos en la LGPDPSO y los Lineamientos Generales.</p>	<ol style="list-style-type: none"> <li>Establecer procedimientos internos para la atención de solicitudes de derechos ARCO conforme a lo previsto por la LGPDPSO y los Lineamientos Generales, sin considerar requisitos adicionales.</li> <li>El procedimiento interno que desarrolle la Unidad de Transparencia para recibir, turnar y responder las solicitudes de ejercicio de derechos ARCO deberá facilitar la presentación de las mismas por parte de los titulares y permitir que las solicitudes se turnen y atiendan internamente de manera eficiente.</li> <li>El procedimiento deberá prever informar a todo el personal de la institución sobre su obligación de conocer la localización de la Unidad de Transparencia para, en su caso, poder brindar orientación al respecto.</li> </ol>	<ul style="list-style-type: none"> <li>Procedimiento para atención de solicitudes de derechos ARCO.</li> </ul>
<ul style="list-style-type: none"> <li>Los medios y procedimientos habilitados para atender las solicitudes para el ejercicio de los derechos ARCO deberán ser de fácil acceso y con la mayor cobertura posible considerando el perfil de los titulares y la forma en que mantienen contacto cotidiano o común con el responsable.</li> </ul>	<ol style="list-style-type: none"> <li>Establecer medios y procedimientos para que los titulares presenten sus solicitudes de ejercicio de derechos ARCO, que sean de fácil acceso, con la mayor cobertura posible y que atiendan al perfil de los usuarios y la forma como se tiene contacto cotidiano o común con ellos.</li> </ol>	<ul style="list-style-type: none"> <li>Medios disponibles para la presentación de solicitudes de ejercicio de derechos ARCO: correo electrónico, PNT, atención personalizada en caso de asistencia en las Oficinas centrales, y atención vía telefónica del personal asignado a la UT.</li> </ul>
<ul style="list-style-type: none"> <li>Establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO.</li> </ul>	<ol style="list-style-type: none"> <li>Elaborar formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, o utilizar aquéllos que haya elaborado el INAI.</li> </ol>	<ul style="list-style-type: none"> <li>Guías elaboradas por la UT.</li> <li>Avisos de privacidad integrales</li> </ul>
<ul style="list-style-type: none"> <li>Procurar que las personas con algún tipo de discapacidad o grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales.</li> </ul>	<ol style="list-style-type: none"> <li>Prever en el procedimiento interno las medidas pertinentes para que las personas con algún tipo de discapacidad o grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales.</li> </ol>	<ul style="list-style-type: none"> <li>Reservar lugares de estacionamiento para personas con discapacidad;</li> <li>Brindar las facilidades para el acceso de perros guías o animales de apoyo;</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
	7. Establecer los acuerdos necesarios con instituciones públicas especializadas que pudieran auxiliar en la recepción, trámite y entrega de las respuestas a solicitudes de ejercicio de derechos ARCO, en la lengua indígena, braille o cualquier formato accesible correspondiente.	<ul style="list-style-type: none"> <li>• Apoyar en la lectura de documentos;</li> <li>• Contar con rampas para personas con discapacidad.</li> <li>• Brindar las facilidades para el acceso y movilidad al interior del Instituto.</li> </ul>

### Trámite de atención

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>• Dar trámite a todas las solicitudes de ejercicio de derechos ARCO y entregar el acuse de recibido que corresponda.</li> <li>• Turnar la Unidad de Transparencia las solicitudes admitidas a las unidades administrativas que puedan poseer los datos personales según sus atribuciones, competencias, facultades o funciones.</li> </ul>	<p>8. El procedimiento interno deberá prever dar trámite a todas las solicitudes y entregar al titular el acuse correspondiente.</p> <p>9. El procedimiento interno deberá prever el turno de las solicitudes a todas las unidades administrativas que pudieran tener los datos personales.</p>	<ul style="list-style-type: none"> <li>• Documentación que acredite la atención de las solicitudes: correos electrónicos y acuses de entrega de información.</li> <li>• Expediente físico y/o electrónico.</li> </ul>
<ul style="list-style-type: none"> <li>• El Infonavit deberá registrar las solicitudes para el ejercicio de los derechos ARCO que se presenten mediante escrito libre en el sistema electrónico habilitado por el INAI.</li> </ul> <p>Remitir solicitud de ejercicio de derechos ARCO de unidad administrativa a Unidad de Transparencia: en caso de que la solicitud para el ejercicio de los derechos ARCO en escrito libre se presente directamente ante una unidad administrativa distinta a la Unidad de Transparencia, la unidad administrativa deberá remitir la solicitud a la Unidad de Transparencia a más tardar al día siguiente de su presentación.</p>	<p>10. Incluir en el procedimiento interno, el registro en el sistema electrónico habilitado por el INAI de las solicitudes que se presenten por escrito libre ante la Unidad de Transparencia, así como lo necesario para su tramitación.</p> <p>11. Incluir en el procedimiento interno, la obligación de la unidad administrativa que reciba una solicitud de ejercicio de derechos ARCO de turnar a la Unidad de Transparencia a más tardar al día siguiente de su presentación.</p> <p>12. Señalar en el procedimiento interno que la solicitud para el ejercicio de los derechos ARCO se tendrá por recibida en la fecha en que fue presentada en la unidad administrativa.</p>	<ul style="list-style-type: none"> <li>• Correos electrónicos al particular.</li> <li>• Expedientes físicos y/o electrónicos.</li> </ul>

### Requisitos de la solicitud de ejercicio de derechos ARCOP

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>• No imponer mayores requisitos para las solicitudes de ejercicio de los derechos</li> </ul>	17. No establecer en el procedimiento interno mayores	<ul style="list-style-type: none"> <li>• Formatos.</li> <li>• Avisos de privacidad</li> <li>• Notificaciones</li> </ul>



Obligaciones	Actividades para su cumplimiento	Evidencia
ARCO, que los que establece la LGPDPPSO en su artículo 52.	requisitos que los señalados por la LGPDPPSO.  18. Prever en el procedimiento interno la verificación de que las solicitudes cumplan con los requisitos que establece el artículo 52 de la LGPDPPSO o, en caso contrario, emitir la prevención que se señala más adelante.	
<ul style="list-style-type: none"> <li>En el caso de solicitudes para el ejercicio del derecho de acceso, el titular podrá acompañarla del medio magnético, electrónico o el mecanismo a través del cual requiere la reproducción de sus datos.</li> <li>En el caso de las solicitudes de rectificación, el titular podrá aportar la documentación que sustente la modificación solicitada.</li> <li>En todos los casos, el titular podrá aportar las pruebas que estime pertinentes para acreditar la procedencia de su solicitud, las cuales deberán acompañar la solicitud desde su presentación.</li> </ul>	<p>19. Prever en el procedimiento interno la recepción de las pruebas y documentación que aporte el titular en sus solicitudes.</p> <p>Con independencia de lo anterior, no se podrá exigir la presentación de esta documentación o pruebas para la procedencia de la solicitud de ejercicio de derechos ARCO.</p>	<ul style="list-style-type: none"> <li>Expedientes de gestión de solicitudes de ejercicio de derechos ARCO.</li> </ul>
<ul style="list-style-type: none"> <li>Prevenir al solicitante, en caso de que la solicitud de ejercicio de derechos ARCO no satisfaga alguno de los requisitos normativos, y no cuenten con elementos para subsanarla, dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio de derechos ARCO, por una sola ocasión, para que subsane las omisiones dentro de un plazo de diez días contados a partir del día siguiente al de la notificación.</li> <li>Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de ejercicio de derechos ARCO.</li> <li>La prevención tendrá el efecto de interrumpir el plazo para resolver la solicitud de ejercicio de los derechos ARCO.</li> </ul>	<p>20. Prever en el procedimiento interno las reglas y plazos para la prevención.</p>	<ul style="list-style-type: none"> <li>Documentación que se genere en la atención de las solicitudes de ejercicio de derechos ARCO.</li> <li>Expediente físico y/o electrónico.</li> </ul>

## Costos

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>El ejercicio de los derechos ARCO debe ser gratuito.</li> </ul>	<p>21. Prever en el procedimiento interno que la atención del ejercicio de los derechos ARCO deberá ser gratuita y sólo se</p>	<ul style="list-style-type: none"> <li>Documentación que se genere con relación a la atención de las solicitudes de</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Sólo pueden realizarse cobros para recuperar los costos de reproducción, certificación o envío.</li> <li>No cobrar reproducción cuando el titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales.</li> <li>La reproducción de los datos personales en copias simples o certificadas será gratuita cuando no excedan de veinte hojas, o bien, las primeras veinte hojas reproducidas o certificadas.</li> </ul>	<p>deberán realizar los cobros que prevé la LGPDPPSO.</p>	<p>ejercicio de derechos ARCOP.</p> <ul style="list-style-type: none"> <li>Ficha de Depósito Referenciado (DEPOREF).</li> <li>Resolución del CT sesión ordinaria 144, con la que se aprueba la modificación del costo de reproducción de las copias certificadas, copias simples y discos compactos.</li> </ul>
<p>La Unidad de Transparencia podrá exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas del titular.</p> <p>Cuando el titular no pueda cubrir los costos de reproducción y/o envío deberá manifestarlo en su solicitud.</p>	<p>22. Incluir en los formatos de solicitudes de ejercicio de derechos ARCO un espacio para que el titular pueda manifestar la circunstancia de no poder cubrir los costos de reproducción y envío.</p> <p>23. Prever en el procedimiento interno que cuando ello se manifieste en una solicitud, se deberá realizar el análisis correspondiente, a fin de determinar si procede la excepción del pago.</p>	<ul style="list-style-type: none"> <li>Formatos para ejercicio de los derechos ARCO.</li> </ul>

### Acreditación de la identidad

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Acreditar la identidad del solicitante de ejercicio de derechos ARCO y, en su caso, la identidad y personalidad de su representante, al momento de que se presente la solicitud o previo a hacer efectivo el derecho correspondiente.</li> </ul> <p>El titular podrá acreditar su identidad con identificación oficial.</p> <p>El representante acreditará su identidad y personalidad con:</p> <ul style="list-style-type: none"> <li>Copia simple de la identificación oficial del titular;</li> <li>Identificación oficial del representante, e</li> <li>Instrumento público; carta poder simple firmada ante dos testigos anexando copia simple de las identificaciones oficiales de quienes intervengan en la suscripción del</li> </ul>	<p>24. Prever en el procedimiento interno que la acreditación de la identidad del titular y, en su caso, de su representante, así como la personalidad de este último, se realice al momento de que se presente la solicitud o previo a hacer efectivo el derecho correspondiente.</p> <p>25. Prever en el procedimiento interno que en la constancia que acredite el ejercicio del derecho de que se trate, se señale que el titular o su representante acreditaron su identidad y personalidad en el caso de este último, mediante la presentación de documentos originales, y describir estos últimos.</p>	<ul style="list-style-type: none"> <li>Documentación generada para acreditar la identidad del titular y, en su caso, la identidad y personalidad de su representante.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
<p>mismo, o declaración en comparecencia personal del titular.</p> <p>La acreditación de la identidad y personalidad se deberá llevar a cabo presentando los documentos originales, en el caso de que el titular o su representante acudan directamente ante la Unidad de Transparencia.</p>		

### *Acreditación de la identidad de menores de edad y personas en estado de interdicción o incapacidad conforme leyes civiles*

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>En el ejercicio de los derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad de conformidad con las leyes civiles, vivos, se estará a las reglas de representación del Código Civil Federal y demás disposiciones jurídicas aplicables.</li> </ul> <p>La identidad de los menores de edad se podrá acreditar mediante su acta de nacimiento, Clave Única de Registro de Población, credenciales expedidas por instituciones educativas o instituciones de seguridad social, pasaporte, o cualquier otro documento oficial utilizado para tal fin.</p> <p>La identidad de personas en estado de interdicción o incapacidad declarada por ley se podrá acreditar mediante su acta de nacimiento, Clave Única de Registro de Población, pasaporte o cualquier otro documento o identificación oficial expedida para tal fin.</p>	<p>26. Prever en el procedimiento interno que se deberán atender las reglas de representación del Código Civil Federal y demás disposiciones jurídicas aplicables.</p>	<ul style="list-style-type: none"> <li>Documentación que se genere para acreditar el ejercicio del derecho que corresponda.</li> </ul>

### *Datos personales de persona fallecida*

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Tratándose de datos personales de una persona fallecida, la persona que acredite tener un interés jurídico de conformidad con las leyes aplicables podrá ejercer los derechos ARCO.</li> </ul> <p>En caso de que la persona fallecida no hubiere expresado fehacientemente su voluntad para que cierta persona ejerza los derechos ARCO con relación a sus datos personales, bastará que la persona que pretende ejercer los derechos ARCO acredite su interés jurídico.</p>	<p>27. Prever en el procedimiento interno que para el ejercicio de derechos ARCO sobre datos personales correspondientes a una persona fallecida, se deberá solicitar a quien pretenda ejercer el derecho, que acredite que el titular de los datos personales hubiere expresado fehacientemente su voluntad de que dicha persona pueda ejercer los derechos ARCO con relación a su información personal, o bien, se confirma que exista interés</p>	<ul style="list-style-type: none"> <li>Documentación que se genere para acreditar el ejercicio del derecho que corresponda.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
<p>En el supuesto de que el titular sea un menor de edad, el interés jurídico se acreditará con la copia del acta de defunción del menor, el acta de nacimiento o identificación del menor, así como la identificación de quien ejercía la patria potestad y/o tutela:</p> <p>En el supuesto de que el titular sea una persona en estado de interdicción o incapacidad declarada por ley o por autoridad judicial, el interés jurídico se acreditará con la copia de su acta de defunción, el documento de su identificación oficial y de quien ejercía la tutela, así como el instrumento legal de designación del tutor.</p> <p>La persona que acredite tener un interés jurídico deberá presentar los siguientes documentos:</p> <ul style="list-style-type: none"> <li>• Acta de defunción del titular;</li> <li>• Documentos que acrediten el interés jurídico de quien pretende ejercer el derecho, y</li> <li>• Documento de identificación oficial de quien solicita el ejercicio de los derechos ARCO.</li> </ul>	<p>jurídico según las reglas señaladas en la columna anterior.</p>	

### Requisitos generales de las respuestas

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>• En la respuesta a una solicitud para el ejercicio de los derechos ARCO, el responsable deberá señalar: <ul style="list-style-type: none"> <li>◦ Los costos de reproducción, certificación y/o envío de los datos personales o de las constancias que acrediten el ejercicio efectivo de los derechos ARCO que, en su caso, correspondan;</li> <li>◦ El plazo que tiene el titular para realizar el pago, no podrá ser menor de tres días contados a partir del día siguiente de que se notifique la respuesta; señalando que una vez que el titular o, en su caso, su representante realice el pago deberá remitir copia del recibo correspondiente, con la identificación del número de folio de la solicitud para el ejercicio de los derechos ARCO que corresponda, a más tardar al día siguiente de realizarse el pago a través del medio que señaló para oír y recibir notificaciones, o bien, presentando personalmente una copia ante la Unidad de Transparencia del Infonavit, y</li> </ul> </li> </ul>	<p>28. Prever en el procedimiento interno la inclusión de los elementos señalados en la columna anterior en las respuestas que se emitan.</p> <p>29. Prever en el procedimiento interno la notificación de las respuestas por los medios permitidos por la norma.</p>	<ul style="list-style-type: none"> <li>• Respuestas emitidas a las solicitudes de ejercicio de derechos ARCO.</li> <li>• Expediente físico y/o electrónico</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>El derecho que le asiste al titular para interponer un recurso de revisión ante el INAI en caso de inconformidad por la respuesta recibida.</li> </ul> <p>La respuesta puede ser notificada a través de los siguientes medios:</p> <ul style="list-style-type: none"> <li>Unidad de Transparencia;</li> <li>Oficina habilitada;</li> <li>Plataforma Nacional (no procede notificación a través de representante), y</li> <li>Correo certificado (Sólo procederá el envío por correo certificado de los datos personales o de las constancias del ejercicio efectivo de los derechos ARCO, cuando la solicitud sea presentada personalmente por el titular ante el responsable, no medie representación alguna del titular, y no se trate de menores de edad o de datos personales de fallecidos).</li> </ul> <p>Cuando el titular o su representante hayan acreditado su identidad y personalidad directamente ante la Unidad de Transparencia, mediante la presentación de documentos originales, la respuesta podrá ser notificada a través de los medios electrónico que haya determinado el titular cuando acudió directamente antes la Unidad de Transparencia.</p>		
<ul style="list-style-type: none"> <li>Se deberá tener a disposición del titular y, en su caso, de su representante los datos personales en el medio de reproducción solicitado y/o las constancias que acrediten el ejercicio efectivo de los derechos ARCO durante un plazo máximo de 60 días, contados a partir del día siguiente en que se hubiere notificado la respuesta de procedencia al titular.</li> </ul> <p>Transcurrido el plazo, el responsable deberá dar por concluida la atención a la solicitud para el ejercicio de los derechos ARCO y proceder a la destrucción del material en el que se reprodujeron los datos personales o de las constancias que acrediten el ejercicio efectivo de los derechos ARCO.</p>	<p>30. Prever en el procedimiento interno mantener a disposición el medio de reproducción con los datos solicitados y las constancias de ejercicio, por un plazo de 60 días, y transcurrido dicho plazo sin que el titular o el responsable los hayan recogido, su eliminación por un medio seguro.</p>	<ul style="list-style-type: none"> <li>Constancia de eliminación en el plazo de 60 días.</li> </ul>

### Cumplimiento del ejercicio de los derechos ARCO

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>La obligación de <b>acceso</b> a los datos personales se dará por cumplida cuando el responsable ponga a</li> </ul>	<p>31. Prever en el procedimiento interno dar acceso a los datos personales en el plazo de 15 días contados a partir del día siguiente a que se haya notificado la</p>	<ul style="list-style-type: none"> <li>Documentación que se genere en la atención de las solicitudes.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
<p>disposición del titular, los datos personales a través de consulta directa, en el sitio donde se encuentren, o mediante la expedición de copias simples, copias certificadas, medios magnéticos, ópticos, sonoros, visuales u holográficos, o cualquier otra tecnología que determine el titular, dentro del plazo de quince días, así como previa acreditación del pago de los derechos correspondientes.</p>	<p>respuesta al titular, en los medios señalados en la columna anterior, una vez acreditada la identidad del titular o de su representante y la personalidad de este último; y verificado el pago de los costos de reproducción y envío correspondientes, en su caso.</p>	<ul style="list-style-type: none"> <li>Expediente físico y/o electrónico</li> </ul>
<ul style="list-style-type: none"> <li>La obligación de <b>rectificar</b> los datos personales se dará por cumplida cuando el responsable notifique al titular, una constancia que acredite la corrección solicitada, dentro del plazo de quince días.</li> </ul> <p>En la constancia, el responsable deberá señalar, al menos:</p> <ul style="list-style-type: none"> <li>El nombre completo del titular,</li> <li>Los datos personales corregidos, y</li> <li>La fecha a partir de la cual fueron rectificadas los datos personales en sus registros, archivos, sistemas de información, expedientes, bases de datos o documentos en su posesión.</li> </ul>	<p>32. Prever en el procedimiento interno la generación de la constancia que acredite la rectificación de los datos personales, en la que se registre la información señalada en la columna anterior, así como la notificación al titular o su representante, previa acreditación de la identidad y, en su caso, personalidad de este último, en el plazo de 15 días contados a partir del día siguiente a que se haya notificado la respuesta al titular.</p>	<ul style="list-style-type: none"> <li>Constancia de rectificación de los datos personales.</li> <li>Base de datos en la que se rectificaron los datos personales.</li> </ul>
<ul style="list-style-type: none"> <li>La obligación de <b>cancelar</b> los datos personales se dará por cumplida cuando el responsable notifique al titular, una constancia que señale:</li> </ul> <ul style="list-style-type: none"> <li>Los documentos, bases de datos personales, archivos, registros, expedientes y/o sistemas de tratamiento donde se encuentren los datos personales objeto de cancelación;</li> <li>El periodo de bloqueo de los datos personales, en su caso;</li> <li>Las medidas de seguridad de carácter administrativo, físico y técnico implementadas durante el periodo de bloqueo, en su caso, y</li> <li>Las políticas, métodos y técnicas utilizadas para la supresión definitiva de los datos personales, de tal manera que la probabilidad de</li> </ul>	<p>33. Prever en el procedimiento interno la generación de la constancia que contenga la información señalada en la columna anterior, y la notificación al titular o su representante, previa acreditación de la identidad y personalidad, en el plazo de 15 días contados a partir del día siguiente a que se haya notificado la respuesta al titular.</p>	<ul style="list-style-type: none"> <li>Constancia de cancelación.</li> <li>Bloqueo de los datos personales.</li> <li>Medidas de seguridad implementadas para el bloqueo y supresión de los datos personales.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
<p>recuperarlos o reutilizarlos sea mínima.</p> <p>El responsable deberá notificar al titular la constancia dentro del plazo de 15 días.</p>		
<ul style="list-style-type: none"> <li>La obligación de <b>oposición</b> al tratamiento de los datos personales se dará por cumplida cuando el responsable notifique al titular, una constancia que señale dicha situación dentro del plazo de 15 días.</li> </ul>	<p>34. Prever en el procedimiento interno la generación de una constancia que se notifique al titular o su representante, previa acreditación de identidad y personalidad, en la que se informe sobre el cese en el tratamiento de datos personales, en el plazo de 15 días contados a partir del día siguiente a que se haya notificado la respuesta al titular.</p>	<ul style="list-style-type: none"> <li>Constancia de ejercicio del derecho de oposición.</li> <li>Información que se genere del uso de la base de datos, en la que conste la eliminación de los datos personales o en la que se demuestre que los datos ya no son tratados para finalidades en lo particular.</li> </ul>

### Modalidad de entrega

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Atender la solicitud de ejercicio del derecho de acceso, en la modalidad requerida por el titular, salvo que exista una imposibilidad física o jurídica, en este caso deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación.</li> </ul>	<p>35. Prever en el procedimiento interno que en el ejercicio del derecho de acceso, se deberá atender la modalidad de reproducción solicitada por el titular, salvo que exista una imposibilidad física o jurídica.</p> <p>En ese caso, se deberán ofrecer otras modalidades, y justificar y motivar esta acción.</p>	<ul style="list-style-type: none"> <li>Documentación que se genere en la atención de las solicitudes de ejercicio del derecho de acceso a datos personales.</li> <li>Expediente físico y/o electrónico</li> </ul>

### Incompetencia

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Hacer del conocimiento del solicitante cuando el Infonavit no sea competente para atender la solicitud para el ejercicio de derechos ARCO, dentro de los 3 días siguientes a la presentación de la solicitud, y en caso de poderlo determinar, orientarlo hacia el responsable competente.</li> <li>Si el Infonavit es competente para atender parcialmente la solicitud, deberá dar respuesta en el ámbito de sus competencias en el plazo de 20 días.</li> <li>En caso de que el Infonavit declare inexistencia de los datos personales, dicha</li> </ul>	<p>36. Prever en el procedimiento interno el plazo de 3 días siguientes a la presentación de la solicitud para hacer del conocimiento del titular cuando el Infonavit no sea competente para atender la solicitud, así como la orientación al sujeto obligado competente, en caso de ser posible.</p> <p>37. Prever en el procedimiento interno la solicitud de declaración formal de la inexistencia de los datos personales por parte del Comité de Transparencia.</p> <p>38. Prever en el procedimiento interno la reconducción de la vía haciéndolo del conocimiento del titular, dentro de los 3 días siguientes a la presentación de la solicitud, en caso de que se advierta que la solicitud para el ejercicio de derechos</p>	<ul style="list-style-type: none"> <li>Documentación generada en la atención de las solicitudes de ejercicio de derechos ARCO.</li> <li>Expediente físico y/o electrónico</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
<p>declaración deberá constar en una resolución del Comité de Transparencia que confirme la inexistencia de los datos personales, y en la que se informen los elementos mínimos para que permitan al titular tener la certeza de que se utilizó un criterio de búsqueda exhaustivo; se señalen las circunstancias de tiempo, modo y lugar que generaron la inexistencia y se identifique la unidad administrativa competente para contar con los datos personales.</p> <ul style="list-style-type: none"> <li>En caso de que se advierta que la solicitud para el ejercicio de derechos ARCO corresponda a un derecho diferente de los previstos en la LGPDPPSO y Lineamientos Generales, deberá reconducir la vía haciéndolo del conocimiento al titular, dentro de los 3 días siguientes a la presentación de la solicitud, dejando a salvo los requisitos y plazos establecidos en la vía correcta conforme a la normatividad aplicable.</li> </ul>	<p>ARCO corresponda a un derecho diferente.</p>	

### Negativa

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Sólo se podrá negar el ejercicio de los derechos ARCO cuando se actualicen algunas de las causas, previstas en el artículo 55 de la LGPDPPSO.</li> <li>Cuando se niegue el ejercicio de los derechos ARCO, la negativa deberá constar en una resolución del Comité de Transparencia en la que confirme la improcedencia.</li> <li>Se deberá informar al titular el motivo de la negativa, en el plazo de hasta veinte días, por el mismo medio en que se llevó a cabo la solicitud, acompañando en su caso, las pruebas que resulten pertinentes.</li> </ul>	<p>39. Negar el ejercicio de los derechos ARCO solo cuando se actualice alguna de las causales previstas en el artículo 55 de la LGPDPPSO.</p> <p>40. Prever en el procedimiento interno informar al titular sobre la negativa para el ejercicio del derecho ARCO que corresponda en el plazo de 20 días hábiles constados a partir del día siguiente a la recepción de la solicitud.</p>	<ul style="list-style-type: none"> <li>Documentación que se genere en la atención de las solicitudes de ejercicio de derechos ARCO.</li> <li>Expediente físico y/o electrónico</li> </ul>



### Trámite específico

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>• Cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un trámite o procedimiento específico para solicitar el ejercicio de los derechos ARCO, se deberá informar al titular sobre la existencia del mismo, en un plazo no mayor a cinco días siguientes a la presentación de la solicitud para el ejercicio de los derechos ARCO, a efecto de que este último decida si ejerce sus derechos a través del trámite específico, o bien, por medio del procedimiento que el Infonavit cuenta para la atención de solicitudes para el ejercicio de los derechos ARCO.</li> </ul> <p>El titular tendrá un plazo de cinco días contados a partir del día siguiente de recibir la respuesta del Infonavit, para indicar si ejerce sus derechos ARCO a través del trámite específico o del procedimiento de la LGPDPPSO. Si el titular no responde, se entenderá que señala el procedimiento general.</p>	<p>41. Prever en el procedimiento interno los plazos y reglas establecidos para informar al titular sobre un trámite distinto para el ejercicio de sus derechos ARCO.</p>	<ul style="list-style-type: none"> <li>• Documentación que se genere en la atención de las solicitudes de ejercicio de derechos ARCO:</li> <li>• Notificaciones de elección.</li> <li>• Apartado de protección de datos personales.</li> <li>• Expediente físico y/o electrónico.</li> </ul>

### Portabilidad

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>• Otorgar al titular una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado</li> </ul>	<p>1. Atender las solicitudes del ejercicio del derecho de portabilidad según los criterios y parámetros establecidos por la LGPDPPSO y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.</p>	<ul style="list-style-type: none"> <li>• Documentación que se genere para atender las solicitudes de ejercicio del derecho de portabilidad.</li> <li>• Expediente físico y/o electrónico</li> </ul>

### Obligaciones en la etapa de eliminación:

#### Supresión de los datos personales (calidad)

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>• Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades y una</li> </ul>	<p>1. Tener identificados los plazos de conservación de las series documentales que contienen datos personales.</p>	<ul style="list-style-type: none"> <li>• Instrumentos de clasificación archivística.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
vez que concluya su plazo de conservación establecido.	2. Realizar la eliminación de los documentos correspondientes a dichas series documentales cuando haya concluido el plazo de conservación respectivo.	<ul style="list-style-type: none"> <li>Evidencia generada en la eliminación de los documentos.</li> <li>Inventario de datos personales</li> </ul>
<ul style="list-style-type: none"> <li>Previo a la supresión procederá el bloqueo.</li> </ul>	3. Considerar en el plazo de conservación y en el procedimiento de archivos, la etapa de bloqueo de los datos personales.	<ul style="list-style-type: none"> <li>Procedimiento de archivo que incluye el bloqueo.</li> </ul>
<ul style="list-style-type: none"> <li>Establecer políticas, métodos y técnicas orientadas a la supresión definitiva de los datos personales, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.</li> </ul> <p>En las políticas, métodos y técnicas, se deberá considerar, al menos, los siguientes atributos y el o los medios de almacenamiento, físicos y/o electrónicos en los que se encuentren los datos personales:</p> <ol style="list-style-type: none"> <li>I. <b>Irreversibilidad:</b> que el proceso utilizado no permita recuperar los datos personales;</li> <li>II. <b>Seguridad y confidencialidad:</b> que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la LGPDPPSO y los Lineamientos Generales, y</li> </ol> <ul style="list-style-type: none"> <li><b>Favorable al medio ambiente:</b> que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.</li> </ul>	4. Establecer las políticas, métodos y técnicas orientadas a la supresión definitiva de los datos personales, considerando los atributos de irreversibilidad; seguridad y confidencialidad y favorable al medio ambiente.	<ul style="list-style-type: none"> <li>Políticas, métodos y técnicas desarrolladas.</li> <li>Documentación y evidencia que se genere con su implementación.</li> </ul>

## Obligaciones transversales:

### Seguridad

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Establecer y mantener <b>medidas de seguridad</b> de carácter administrativo, físico y técnico, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad e impedir que cualquier tratamiento contravenga las</li> </ul>	1. Establecer y mantener medidas de seguridad administrativas, técnicas y físicas para la protección de los datos personales, a partir de las acciones que se describen en esta sección.	<ul style="list-style-type: none"> <li>Programa de seguridad.</li> <li>Documento de seguridad.</li> <li>Evidencia generada en la implementación de los controles de seguridad.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
disposiciones del marco normativo en la materia.		
<ul style="list-style-type: none"> <li>Tomar en cuenta otras disposiciones vigentes en materia de seguridad de la información emitidas por otras autoridades, cuando éstas contemplen una mayor protección para el titular o complementen lo dispuesto por la LGPDPPSO y los Lineamientos Generales.</li> </ul>	2. Revisar el marco normativo que regula el tratamiento específico de los datos personales, a fin de identificar medidas de seguridad adicionales y analizar la procedencia de su implementación.	<ul style="list-style-type: none"> <li>Marco normativo que regula en lo particular el tratamiento en cuestión.</li> </ul>
<p><b>Políticas internas:</b></p> <ul style="list-style-type: none"> <li>Crear <b>políticas internas</b> para la gestión y tratamiento de los datos personales.</li> </ul>	Reuniones de trabajo.	<ul style="list-style-type: none"> <li>Política de tratamiento y gestión de datos personales.</li> </ul>
<ul style="list-style-type: none"> <li>Crear <b>políticas internas</b> para la seguridad de la información, entre ésta los datos personales.</li> </ul>	Reuniones de trabajo	<ul style="list-style-type: none"> <li>Políticas Institucionales para Seguridad de la Información</li> </ul>
<p><b>Funciones del personal que trata datos personales:</b></p> <ul style="list-style-type: none"> <li>Establecer y documentar las funciones, obligaciones y cadena de rendición de cuentas del personal involucrado en el tratamiento de datos personales.</li> <li>Establecer mecanismos para asegurar que el personal involucrado en el tratamiento de datos personales conozca sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento</li> </ul>	<p>Definir las funciones, obligaciones y cadena de mando del personal que trate datos personales, por unidad administrativa.</p> <p>5. Comunicar al personal la información antes señalada, así como capacitarlos en la materia.</p>	<ul style="list-style-type: none"> <li>Documento en el que se establezcan las funciones, obligaciones y cadena de mando de cada empleado por unidad administrativa, que trate datos personales.</li> <li>Documento mediante el cual se haya comunicado la información antes señalada.</li> </ul>
<p><b>Inventario:</b></p> <ul style="list-style-type: none"> <li>Elaborar un inventario de datos personales y de los sistemas de tratamiento.</li> </ul>	6. Elaborar el inventario de datos personales y de los sistemas de tratamiento.	<ul style="list-style-type: none"> <li>Inventario de datos personales.</li> <li>Registro</li> </ul>
<p><b>Análisis de riesgos y brecha y plan de trabajo:</b></p> <ul style="list-style-type: none"> <li>Realizar un análisis de riesgo de los datos personales.</li> </ul>	7. Elaborar el análisis de riesgo tomando en cuenta los elementos señalados en la columna anterior.	<ul style="list-style-type: none"> <li>Análisis de riesgo documentado.</li> <li>Documento de seguridad.</li> </ul>
Realizar un análisis de brecha	8. Realizar el análisis de brecha con los elementos señalados en la columna anterior.	<ul style="list-style-type: none"> <li>Análisis de brecha documentado.</li> <li>Documento de seguridad.</li> </ul>
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.	9. Elaborar el plan de trabajo después de contar con el análisis de riesgo y de brecha, priorizando las medidas de seguridad más relevantes y urgentes.	<ul style="list-style-type: none"> <li>Plan de trabajo elaborado.</li> <li>Documentos de análisis de riesgo y de brecha.</li> </ul>
Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y	10. Elaborar un plan de monitoreo periódico de las medidas de seguridad implementadas, las amenazas y las	<ul style="list-style-type: none"> <li>Plan de monitoreo periódico.</li> <li>Documentación que se genere a partir de la</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
vulneraciones a las que están sujetos los datos personales.	vulnerabilidades a las que estén sujetos los datos personales.  11. Implementar el plan de monitoreo periódico.	implementación del plan.
Diseñar y aplicar cursos de <b>capacitación</b> al personal	<ul style="list-style-type: none"> <li>Desarrollar temario</li> <li>Implementar plataforma o herramienta para desarrollar los cursos.</li> </ul>	<ul style="list-style-type: none"> <li>Bases de datos de personal capacitado</li> <li>Evidencia de curso realizado</li> </ul>
Diseñar y aplicar diferentes niveles de <b>capacitación</b> del personal respecto del tratamiento de los datos personales.	<ul style="list-style-type: none"> <li>Desarrollar temario</li> <li>Implementar plataforma o herramienta para desarrollar los cursos.</li> </ul>	<ul style="list-style-type: none"> <li>Bases de datos de personal capacitado</li> <li>Evidencia de curso realizado</li> </ul>
Implementar un <b>sistema de gestión para la seguridad de los datos personales.</b>	13. Implementar el presente Programa que se basa en un sistema de gestión integral, que no solamente abarca medidas de seguridad específicas, sino la totalidad de obligaciones previstas en la LGPDPPSO y los Lineamientos Generales.	<ul style="list-style-type: none"> <li>Programa.</li> <li>Documentación que se genere a partir de la implementación del Programa.</li> </ul>
<ul style="list-style-type: none"> <li>Elaborar un <b>Documento de seguridad</b></li> </ul>	14. Elaborar el Documento de seguridad con la información antes señalada.	<ul style="list-style-type: none"> <li>Documento de seguridad.</li> </ul>
<p>Actualizar el documento de seguridad cuando ocurran los siguientes eventos:</p> <ul style="list-style-type: none"> <li>Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;</li> <li>Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;</li> <li>Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, e</li> <li>Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.</li> </ul>	15. Actualizar el documento de seguridad cuando ocurra alguno de los supuestos antes señalados.	<ul style="list-style-type: none"> <li>Documento de seguridad.</li> </ul>

## Vulneraciones

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Informar al titular de los datos personales y al INAI, las vulneraciones que afecten</li> </ul>	1. Contar con mecanismos que permitan identificar cuándo ocurrió una vulneración a las bases de datos o archivos.	<ul style="list-style-type: none"> <li>Mecanismos implementados para</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
de forma significativa los derechos patrimoniales o morales, en un plazo máximo de 72 horas, a partir de que se confirme que ocurrió la vulneración y que se haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación.	2. Establecer un procedimiento para notificar las vulneraciones ocurridas al titular de los datos personales y al INAI en el plazo de 72 horas.	<p>detectar vulneraciones ocurridas.</p> <ul style="list-style-type: none"> <li>Procedimiento para la gestión de vulneraciones de datos personales.</li> </ul>
<ul style="list-style-type: none"> <li>Informar al titular de los datos personales</li> </ul>	<p>3. Elaborar un formato de notificación de las vulneraciones de seguridad ocurridas, donde se incluya la información a la que refiere la columna anterior.</p> <p>4. Realizar las notificaciones de las vulneraciones cuando éstas ocurran, en el momento y con la información antes señalada.</p>	<ul style="list-style-type: none"> <li>Formato de notificación al titular de la vulneración de seguridad ocurrida.</li> <li>Constancia de la notificación</li> </ul>
<ul style="list-style-type: none"> <li>Informar al INAI</li> </ul>	<p>5. Elaborar un formato de notificación de las vulneraciones de seguridad ocurridas, que incluya la información a la que refiere la columna anterior.</p> <p>6. Realizar las notificaciones de las vulneraciones cuando éstas ocurran, en el momento y con la información antes señalada.</p>	<ul style="list-style-type: none"> <li>Oficio con el que se informa al INAI.</li> <li>Herramienta INAI: H-COM</li> <li>Correos electrónicos.</li> </ul>
<ul style="list-style-type: none"> <li>Determinar los medios por los cuales se notificará a los titulares de los datos personales respecto de las vulneraciones ocurridas, tomando en cuenta lo siguiente: el perfil de los titulares, la forma en que se mantiene contacto o comunicación con éstos, que sean gratuitos; de fácil acceso; con la mayor cobertura posible y que estén debidamente habilitados y disponibles en todo momento para el titular.</li> </ul>	7. Determinar los medios de notificación de las vulneraciones.	<ul style="list-style-type: none"> <li>Documento en el que se describan los medios que se utilizarán en caso de que sea necesario notificar vulneraciones.</li> <li>Medio utilizado para notificar la vulneración.</li> </ul>
<ul style="list-style-type: none"> <li>Llevar una <b>bitácora</b> de las vulneraciones de seguridad ocurridas, en la que se describa la vulneración, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.</li> </ul>	<p>1. Elaborar un formato de bitácora de las vulneraciones ocurridas con la información antes señalada.</p> <p>9. Llevar una la bitácora de las vulneraciones de seguridad ocurridas.</p>	<ul style="list-style-type: none"> <li>Bitácoras.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
<p><b>Acciones preventivas y correctivas:</b></p> <p>Analizar las causas por las cuales se presentó la vulneración e implementar en el plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales, a fin de evitar que la vulneración se repita.</p>	<p>10. Identificar y documentar las posibles causas de la vulneración e implementar las acciones preventivas y correctivas que se requieran para evitar que se repita.</p> <p>11. Informar al Comité de Transparencia las acciones implementadas para evitar que se repita la vulneración.</p>	<ul style="list-style-type: none"> <li>• Análisis realizado.</li> <li>• Acciones implementadas.</li> <li>• Informe al Comité de Transparencia.</li> </ul>

### Confidencialidad

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>• Establecer controles o mecanismos para que todas las personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad.</li> </ul>	1. Incluir en las medidas de seguridad, controles para garantizar la confidencialidad de los datos personales.	<ul style="list-style-type: none"> <li>• Documento de seguridad.</li> <li>• Controles definidos para la confidencialidad de los datos personales.</li> </ul>
	2. Implementar los controles para la confidencialidad de los datos personales.	<ul style="list-style-type: none"> <li>• Evidencia de la aplicación de los controles.</li> </ul>
	3. Establecer cláusulas en los contratos con los encargados, que obliguen a la confidencialidad de los datos personales.	<ul style="list-style-type: none"> <li>• Contratos celebrados con los encargados del tratamiento.</li> </ul>
	4. Implementar capacitación para el personal del Instituto, a fin de generar conciencia sobre la importancia de guardar la confidencialidad de los datos personales que tratan.	<ul style="list-style-type: none"> <li>• Evidencia que acredite la capacitación.</li> </ul>

### Otras obligaciones:

#### Responsabilidad

Obligaciones	Actividades para su cumplimiento	Evidencia
<p>Implementar las siguientes acciones para acreditar el cumplimiento de los principios, deberes y obligaciones, así como para rendir cuentas:</p> <ul style="list-style-type: none"> <li>• Autorizar y destinar recursos para la instrumentación de programas y políticas de protección de datos personales.</li> </ul>	1. Prever presupuesto para la instrumentación de programas y políticas de protección de datos personales.	<ul style="list-style-type: none"> <li>• Presupuesto del ejercicio en curso.</li> </ul>
<ul style="list-style-type: none"> <li>• Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización, tomando en cuenta el desarrollo</li> </ul>	<ol style="list-style-type: none"> <li>1. Elaborar políticas de gestión y tratamiento de datos personales.</li> <li>2. Elaborar un programa que contemple el cumplimiento</li> </ol>	<ul style="list-style-type: none"> <li>• Programa</li> <li>• Política de tratamiento y gestión de datos personales</li> <li>• Documentación que avale la aprobación e</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
tecnológico y las técnicas existentes; la naturaleza, contexto, alcance, finalidades del tratamiento, atribuciones y facultades del responsable y demás cuestiones que se consideren convenientes.	obligatorio al interior de la organización del responsable.	implementación de la Política.
<ul style="list-style-type: none"> <li>Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.</li> </ul>	3. Elaborar y aplicar un programa de capacitación y actualización del personal en materia de protección de datos personales, de conformidad con el apartado de Capacitación de este Programa.	<ul style="list-style-type: none"> <li>Programa de capacitación para personal del Infonavit.</li> </ul>
<ul style="list-style-type: none"> <li>Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.</li> <li>Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.</li> </ul> <p>Las revisiones de las políticas y programas de seguridad y del sistema de supervisión y vigilancia implementados se deberá realizar cada dos años, salvo que se realicen modificaciones sustanciales a los tratamientos y sea necesaria una revisión previa.</p>	4. Establecer un sistema de supervisión y vigilancia interna y/o externa para comprobar el cumplimiento de este programa, incluyendo las medidas de seguridad, que prevea una revisión cada dos años o antes si es necesario por un cambio sustancial en el tratamiento.	<ul style="list-style-type: none"> <li>Programa de supervisión y vigilancia, y resultados obtenidos.</li> </ul>
<ul style="list-style-type: none"> <li>Establecer procedimientos para recibir y responder dudas y quejas de los titulares, que sea de fácil acceso y con la mayor cobertura posible, considerando el perfil de los titulares y la forma en que se mantiene contacto o comunicación directa o cotidiana con ellos, así como estar, en todo momento, habilitado.</li> </ul>	5. Establecer un procedimiento para atender dudas y quejas de los titulares con las características señaladas en la columna anterior.	<ul style="list-style-type: none"> <li>Procedimiento establecido.</li> </ul>
<ul style="list-style-type: none"> <li>Implementar mecanismos para evidenciar el cumplimiento de los principios, deberes y obligaciones ante los titulares y el Instituto, tanto de tratamientos propios como de aquéllos realizados por los encargados y en las transferencias nacionales e internacionales.</li> </ul>	7. En todos los casos generar pruebas para acreditar el cumplimiento de los principios, deberes y obligaciones que establece la LGPDPSO, los Lineamientos Generales y demás disposiciones que resulten aplicables.	<ul style="list-style-type: none"> <li>Pruebas generadas según lo establecido en la columna de "Medios para acreditar el cumplimiento" de todos los cuadros de este Programa.</li> </ul>

## Evaluación de impacto en la protección de datos personales

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Realizar una evaluación de impacto en la protección de datos personales, y presentarla ante el área establecida por el INAI cuando se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier tipo de tecnologías que impliquen el tratamiento intensivo o relevante de datos personales.</li> </ul>	<p>1. Establecer un procedimiento que prevea lo siguiente, tomando en cuenta lo establecido en las Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales:</p> <ul style="list-style-type: none"> <li>Los mecanismos para detectar los casos en que se requiera la realización de la Evaluación de Impacto en la Protección de Datos Personales.</li> <li>Los mecanismos para la elaboración y presentación de las Evaluaciones de Impacto en la Protección de Datos Personales.</li> <li>Los medios para la atención de las observaciones que, en su caso, emita el INAI.</li> </ul>	<ul style="list-style-type: none"> <li>Documentación que se genere con motivo de la elaboración de la evaluación.</li> <li>Evaluación de impacto</li> </ul>
<ul style="list-style-type: none"> <li>Atender el plazo para presentar la evaluación ante el INAI: 30 días anteriores a la fecha en que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología.</li> <li>Atender las observaciones que en su caso realice el INAI, y justificar cuando ello no sea posible.</li> </ul>	<p>2. Presentar en tiempo y forma las Evaluaciones que se requieran ante el área que establezca el INAI.</p>	<ul style="list-style-type: none"> <li>Documentación que se genere con motivo de la presentación de la Evaluación ante el INAI y la atención de las observaciones que en su caso emita el Instituto.</li> </ul>

## Funciones del Comité de Transparencia

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales al interior del Infonavit, y al respecto, tendrá las siguientes funciones: <ul style="list-style-type: none"> <li>Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales, de conformidad con las disposiciones previstas en la LGPDPSO y en aquellas disposiciones que resulten aplicables en la materia;</li> </ul> </li> </ul>	<p>1. Establecer un programa de trabajo para la implementación del Programa, el cual será susceptible de ajustarse <b>conforme a las necesidades operativas del Instituto.</b></p> <p>2. Supervisar la debida implementación del Programa por parte de las unidades administrativas y <b>realizar las modificaciones o mejoras al mismo que resulten pertinentes, conforme a las necesidades operativas del Instituto.</b></p> <p>3. Establecer un procedimiento para supervisar el cumplimiento de las medidas de seguridad, controles y</p>	<ul style="list-style-type: none"> <li>Programas establecidos e implementados.</li> <li>Actas de sesiones</li> <li>Resoluciones</li> </ul>



Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>o Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;</li> <li>o 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 ARCO;</li> <li>o Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la LGPDPSO y en aquellas disposiciones que resulten aplicables en la materia;</li> <li>o Supervisar, en coordinación con las unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el Documento de seguridad;</li> <li>o Dar seguimiento y cumplimiento a las resoluciones emitidas por el INAI;</li> <li>o Establecer programas de capacitación y actualización del personal en materia de protección de datos personales, y</li> <li>o Dar vista a la Contraloría General 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.</li> </ul>	<p>acciones previstos en el Documento de seguridad.</p> <p>4. Establecer un programa de capacitación y actualización para el personal, en materia de protección de datos personales, <b>el cual podrá ajustarse conforme a las necesidades operativas del Instituto.</b></p>	

### *Funciones de la Unidad de Transparencia*

Obligaciones	Actividades para su cumplimiento	Evidencia
La Unidad de Transparencia tendrá las siguientes funciones en materia	1. Establecer procedimientos internos para cumplir con sus funciones y para	<ul style="list-style-type: none"> <li>• Procedimientos y programas</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
<p>de protección de datos personales:</p> <ul style="list-style-type: none"> <li>o Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales;</li> <li>o Gestionar las solicitudes para el ejercicio de los derechos ARCO;</li> <li>o Establecer mecanismos para asegurar que los datos personales sólo se entreguen a su titular o su representante debidamente acreditados;</li> <li>o 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;</li> <li>o 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 ARCO;</li> <li>o Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO.</li> <li>o Asesorar a las unidades administrativas en materia de protección de datos personales.</li> </ul>	<p>gestionar de manera eficiente las solicitudes de derechos ARCO.</p> <p>2. Diseñar la metodología y programa de evaluaciones de calidad sobre la gestión de las solicitudes de ejercicio de los derechos ARCO, y aplicar dichas evaluaciones.</p>	<p>establecidos e implementados.</p> <ul style="list-style-type: none"> <li>• Correos electrónicos</li> <li>• Minutas de reuniones de trabajo</li> <li>• Notas técnicas</li> <li>• Opiniones técnicas</li> </ul>
<ul style="list-style-type: none"> <li>• Auxiliar y orientar al titular en la elaboración de las solicitudes para el ejercicio de sus derechos ARCO, en todo momento, y en especial en aquellos casos en que el titular no sepa leer ni escribir, así como informar sobre la obligación del titular de acreditar su identidad y, en su caso, la identidad y personalidad de su representante.</li> <li>• Para el caso de las personas con alguna discapacidad, la Unidad de Transparencia procurará atender a cada uno de los titulares, de acuerdo con su situación particular, facilitando en todo momento la información que éstos</li> </ul>	<p>3. Auxiliar y orientar a los titulares en las presentaciones de sus solicitudes de ejercicio de derechos ARCO.</p>	<ul style="list-style-type: none"> <li>• Procedimientos y programas establecidos e implementados.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
requieran para el ejercicio de sus derechos ARCO.		

### Capacitación

Obligaciones	Actividades para su cumplimiento	Evidencia
<ul style="list-style-type: none"> <li>Establecer un programa anual de capacitación y actualización en materia de protección de datos personales, dirigido tanto a personal como a encargados.</li> </ul> <p>El programa de capacitación deberá considerar los roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de puestos.</p>	<p>1. Establecer un programa anual de capacitación y actualización en materia de protección de datos personales para el personal del Instituto.</p>	<ul style="list-style-type: none"> <li>Programa anual de capacitación en materia de protección de datos personales.</li> </ul>

### Revisiones y auditorías:

Con objeto de monitorear y revisar la eficacia y eficiencia del sistema de gestión en que se basa este Programa vinculante al interior del Infonavit, se deberá contar con un programa para llevar a cabo dos tipos de acciones: 1) revisiones y 2) auditorías.

Las auditorías las deberá realizar un actor externo al Comité de Transparencia; mientras que las revisiones las realizará el propio Comité de Transparencia con el apoyo de la Unidad de Transparencia. Las auditorías podrán ser:

- Internas
- Externas, cuando exista el presupuesto para ello y la importancia del caso lo amerite.
- Voluntarias, realizadas a través del INAI según el artículo 151 de la LGPDPPSO, cuando sea con relación a un tratamiento específico y no a todo el sistema de gestión de los datos personales.

Obligaciones	Actividades para su cumplimiento	Evidencia
El responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.	<p>1. Elaborar un programa de aplicación de las revisiones administrativas y auditorías, el cual formará parte de este Programa.</p> <p>2. Realizar al menos una auditoría integral al programa una vez al año.</p> <p>Las auditorías deberán incluir la revisión del cumplimiento de las obligaciones que tiene el Comité de Transparencia en cuanto a la aplicación de este Programa; evaluar la conformidad con este Programa; incluir, cuando sea posible, cifras, indicadores y estadísticas relacionadas con los procedimientos puestos en operación, y contener</p>	<ul style="list-style-type: none"> <li>Programa de aplicación de revisiones administrativas y auditorías</li> <li>Reportes de las auditorías.</li> <li>Resultados que permitan identificar el nivel de madurez del Infonavit con relación a la protección de datos personales en su posesión.</li> <li>Mecanismos para asegurar la objetividad</li> </ul>

Obligaciones	Actividades para su cumplimiento	Evidencia
	<p>recomendaciones para hacer más efectivo y eficiente el cumplimiento del Programa.</p> <p>Asimismo, se podrán llevar a cabo auditorías parciales cuando resulten necesarias para supervisar y monitorear el cumplimiento de obligaciones específicas en tratamientos particulares.</p> <p>Como resultado de las auditorías se deberá obtener el nivel de madurez del Infonavit con relación a la protección de datos personales en su posesión, a fin de tenerlo como referencia y línea base para la mejora continua</p> <p>En el caso de auditorías externas, el Comité de Transparencia deberá asegurar la objetividad e imparcialidad del auditor y el programa propuesto.</p>	<p>e imparcialidad del auditor y el programa propuesto.</p>
	<p>3. Llevar a cabo revisiones administrativas, las cuales deberán estar documentadas, y tendrán como objetivo supervisar: i) el adecuado desarrollo y efectividad de este Programa, o bien, ii) el debido tratamiento en los cambios que afecten aspectos significativos en la protección de datos personales, como nueva normatividad, tecnología, o procesos o procedimientos.</p> <p>Las revisiones administrativas deberán basarse en:</p> <ul style="list-style-type: none"> <li>• La retroalimentación por parte de las unidades administrativas;</li> <li>• Los riesgos identificados en el análisis de riesgos;</li> <li>• Los resultados de auditorías;</li> <li>• Los resultados de las revisiones anteriores;</li> <li>• Las actualizaciones o cambios en la tecnología, normatividad y procesos aplicables e implementados en el Instituto;</li> <li>• Los requerimientos por parte de autoridades;</li> <li>• Las quejas, y</li> <li>• Las vulneraciones de seguridad.</li> </ul>	<ul style="list-style-type: none"> <li>• Documentos que acrediten la realización de la revisión administrativa.</li> </ul>

### Acciones para la mejora continua

Se adoptarán las medidas preventivas y correctivas que hayan resultado de las auditorías y revisiones realizadas, o bien que se hayan obtenido de otras fuentes de información relevantes.

Los puntos de mejora de la implementación del Programa pueden ser de dos tipos:

1. **Acciones preventivas:** aquellas encaminadas a evitar cualquier “no conformidad” (no cumplimiento) con relación a lo establecido en este Programa.

En las acciones preventivas se deben llevar a cabo las siguientes actividades:

- El análisis y revisión de las posibles causas de no conformidad;

- Determinar las no conformidades que podría desencadenarse a partir de ciertas situaciones de riesgo para el tratamiento de datos personales;
- Evaluar las acciones necesarias para evitar que la no conformidad ocurra;
- Determinar e implementar estas acciones;
- Documentar los resultados de las acciones tomadas, y
- Revisar la eficacia de las acciones preventivas tomadas.

**2. Acciones correctivas:** son aquéllas encaminadas a eliminar las causas de la “no conformidad” con relación a lo previsto en este Programa.

En las acciones correctivas se deben llevar a cabo, al menos, las siguientes actividades:

- Analizar y revisar la no conformidad;
- Determinar las causas que dieron origen a la no conformidad;
- Evaluar las acciones necesarias para evitar que la no conformidad vuelva a ocurrir;
- Implementar estas acciones;
- Documentar los resultados de las acciones tomadas, y
- Revisar la eficacia de las acciones correctivas tomadas.

El objetivo de las acciones correctivas es eliminar la causa de la no conformidad, o bien, reducir su grado de prevalencia.

El Comité de Transparencia deberá establecer un plazo límite para que se corrijan las no conformidades detectadas.

El Comité de Transparencia deberá documentar las medidas preventivas o correctivas realizadas para la mejora continua en la implementación de este Programa.

Obligaciones	Actividades para su cumplimiento	Evidencia
El Infonavit deberá implementar acciones para evitar o corregir cualquier no conformidad.	Elaborar un procedimiento para la gestión de las acciones preventivas y correctivas.	<ul style="list-style-type: none"><li>• Procedimiento para la gestión de acciones preventivas y correctivas.</li><li>• Documentación que acredite las acciones preventivas o correctivas implementadas, así como los resultados y revisiones de las acciones una vez implementadas.</li></ul>

## 4. Roles y responsabilidades

### 4.1 De la Alta Dirección

Para que los objetivos planteados se logren con éxito, el Programa requiere del apoyo e impulso directo del más alto nivel del Instituto, con independencia de las funciones que otorgan los artículos 83 y 84 de la Ley General de Datos al Comité de Transparencia, en su carácter de máxima autoridad de datos personales en la organización.

## 4.2 Del Comité de Transparencia

Los artículos 83 y 84, fracción I de la Ley General de Datos y 47 segundo párrafo, y 48 de los Lineamientos Generales, 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, por lo cual tendrá las siguientes funciones con relación a este programa:

- Elaborar, aprobar, coordinar y supervisar el Programa, en conjunto con las áreas técnicas que estime necesario involucrar o consultar.
- Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación.
- Presentar un informe anual al titular de la institución, en el que se describan las acciones realizadas para cumplir con lo dispuesto por este Programa.
- Supervisar la correcta implementación del Programa.
- Las demás que de manera expresa señale el propio Programa.

## 4.3 De las Unidades administrativas

Las unidades administrativas, con el apoyo de la Unidad de Transparencia, deberán continuar realizando las acciones necesarias para cumplir con las obligaciones que establece este Programa, para lo cual deberán:

- Asignar los recursos materiales, financieros, en su caso, y humanos necesarios.
- Asignar a los enlaces específicos o de transparencia y datos personales para el cumplimiento de requerimientos.
- Cumplir con los requerimientos o las actividades específicas en tiempo y forma.
- Subsanciar las observaciones realizadas por la Unidad de Transparencia.

## 4.4 De los Enlaces de transparencia y datos personales

Los designados como enlaces de transparencia y datos personales, así como aquellos específicos, al interior de sus unidades administrativas, Órganos Colegiados o Sectores deben recibir, turnar y gestionar los requerimientos asignados para el cumplimiento de las obligaciones en datos personales con el propósito de dar atención en tiempo y forma.

De igual manera, en el caso de las unidades administrativas, los enlaces deben cumplir con las funciones previstas en los Lineamientos de Transparencia, Acceso a la Información, Archivos y Protección de Datos Personales del Instituto del Fondo Nacional de la Vivienda para los Trabajadores.

Asimismo, podrán solicitar a la Unidad de Transparencia consulta, acompañamiento o asesoría, para poder dar cumplimiento de las obligaciones de datos personales.

#### 4.5 De la Unidad de Transparencia

Es fundamental que el Programa se conozca al interior del Instituto, por lo que la Unidad de Transparencia deberá:

- En coordinación con la OPDP se encargará de difundirlo entre el personal.
- Elaborar, coordinar y supervisar el Programa con las unidades administrativas y áreas técnicas que estime necesario involucrar o consultar.

#### 4.6 De la Oficial de Protección de Datos Personales

Por su parte la **OPDP**, conforme a los artículos 85 segundo párrafo de la Ley General de Datos, y 121 y 122 de los Lineamientos Generales, respecto al Programa debe:

- Proponer al CT políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley General de Datos y su normatividad derivada.
- Implementar políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley General de Datos.
- Coordinar la implementación del Programa en las unidades administrativas del Infonavit.
- Asesorar a las unidades administrativas en la implementación de este Programa, con el apoyo de las áreas técnicas que estime pertinente.
- Dar a conocer el Programa al interior del Infonavit.

#### 4.7 Del Oficial den Jefe de Seguridad de la Información

Como encargado de vigilar el cumplimiento de las Políticas Institucionales para la Seguridad de la Información proporcionará apoyo a la UT y a la OPDP para elaborar, actualizar e implementar el Programa, así como el o los Documentos de Seguridad que correspondan, de conformidad con las atribuciones que dicho cargo<sup>2</sup> le faculta, principalmente respecto a los deberes de seguridad y confidencialidad en materia de protección de datos personales.

En el mismo sentido, deberá brindar asesoría a las unidades administrativas cuando éstas sometan temas en materia de seguridad y confidencialidad respecto a datos personales, a su consideración.

---

<sup>2</sup> Designación hecha por el Director General del Infonavit, mediante oficio DG/064/2024 el 05 de abril de 2024.

#### 4.8 De las y los trabajadores del INFONAVIT

Para el cumplimiento integral de las obligaciones que establece la Ley General de Datos y los Lineamientos Generales, el Programa será de observancia obligatoria para todo el personal del Infonavit que en el ejercicio de sus funciones traten datos personales.

Todos los trabajadores y trabajadoras del Instituto, personal de los órganos Colegiados y de los Sectores, así como los prestadores de servicios y encargados que, en el ejercicio de sus funciones traten datos personales deberán observar, de manera obligatoria, lo señalado en el Programa con la finalidad de que tengan como resultado el cumplimiento integral de las obligaciones que establece la Ley General de Datos y su normativa derivada.

El personal debe contar la capacitación mínima, sobre datos personales previstos en Universidad Infonavit.

#### 4.9 De los encargados

Deben apegarse a lo instruido por el INFONAVIT, siempre cumpliendo lo previsto en los contratos correspondientes, así como con la normativa que le sea aplicable y las Políticas Institucionales para Seguridad de la información y la Política de tratamiento y gestión de datos personales.

#### 4.10 De la Subdirección General de Tecnologías de Información

Se sumará al cumplimiento del Programa de manera específica en materia de desarrollo y uso de tecnologías de información y gestión de la seguridad de la información, conforme a las atribuciones que le están indicadas en apego al Estatuto Orgánico del Infonavit.

Durante septiembre de 2024, la Unidad de Transparencia realizó trabajos con la SGTI para lograr la reconfiguración de una herramienta informática que contenga el Inventario Institucional de Datos Personales, la cual permita tener una organización y trazabilidad de los datos personales, bases de datos y de los sistemas con datos personales, lo que abonará a la gobernanza de datos, así como a la seguridad y confidencialidad de la información personal que trata el Instituto conforme a la Ley General de Datos y su normativa derivada.

Dicha herramienta permitirá identificar, ubicar y organizar los datos personales a fin de que sirva para la toma de mejores decisiones institucionales sustantivas y operativas, con seguridad, calidad y responsabilidad.



## 5. Causas de sanción

Para esta edición, se continua con las causas de sanción previstas en el artículo 163 de la Ley General de Datos.

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 el personal que está a cargo del tratamiento de datos personales tenga presente que de conformidad con el artículo 163 de la LGPDPSO serán causas de sanción por incumplimiento de las obligaciones establecidas en dicha ley, las siguientes:

- Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO.
- Incumplir los plazos de atención previstos en la Ley General de Datos para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate.
- 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.
- Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la Ley General de Datos.
- 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 Ley General de Datos, según sea el caso, y demás disposiciones que resulten aplicables en la materia.
- 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.
- Incumplir el deber de confidencialidad establecido en el artículo 42 de la Ley General de Datos.
- No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la Ley General de Datos.
- Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la Ley General de Datos.
- Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la Ley General de Datos.
- Obstruir los actos de verificación de la autoridad.

- Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la Ley General de Datos.
- No acatar las resoluciones emitidas por el INAI.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, y XII, así como la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves. Cabe destacar que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

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 a Contraloría y, en su caso, dé inicio el procedimiento de responsabilidad administrativo respectivo.

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.

El Comité de Transparencia, a través de la Unidad de Transparencia, tomará las medidas necesarias para dar a conocer esta información a las y los trabajadores y trabajadoras, prestadores de servicio, y quienes intervengan en cualquier tipo de tratamiento de los datos personales al interior del Instituto.

### **Asesoría y acompañamiento**

El presente Programa ha sido elaborado por la Unidad de Transparencia, para la atención de cualquier duda al respecto, acércate a la Unidad de Transparencia [unidadtransparencia@infonavit.org.mx](mailto:unidadtransparencia@infonavit.org.mx) , [jlojero@infonavit.org.mx](mailto:jlojero@infonavit.org.mx) y/o a la OPDP [khernandezc@infonavit.org.mx](mailto:khernandezc@infonavit.org.mx)