



DESARROLLO TERRITORIAL

SECRETARÍA DE DESARROLLO AGRARIO, TERRITORIAL Y URBANO

INSUS

INSTITUTO NACIONAL
DEL SUELO SUSTENTABLE

**PROGRAMA DE PROTECCIÓN DE DATOS
PERSONALES EN POSESIÓN DEL INSTITUTO
NACIONAL DEL SUELO SUSTENTABLE
2024**





Contenido

Presentación	3
Marco normativo.....	4
Glosario	6
Principios del Tratamiento de Datos Personales.....	9
Objetivo General del Programa	11
Objetivos específicos del Programa	11
Responsables de la implementación del Programa	11
o Comité de Transparencia	11
o Unidad de Transparencia (UT):	12
Alcance del Programa.....	14
Identificación y Categorización de Datos Personales	15
Ciclo de vida de los Datos Personales.....	16
Responsables del Tratamiento de Datos Personales.....	17
Respuesta a incidentes o vulneraciones de seguridad	26
Sanciones	27



Presentación

Este programa se elabora para dar cumplimiento a los artículos 30, fracciones I, y II, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y 47 de los Lineamientos Generales para Protección de Datos Personales en el Sector Público, los cuales establecen que, entre las acciones que deberán realizar los responsables del tratamiento de datos personales para cumplir con el principio de responsabilidad, está la elaboración de políticas y programas de protección de datos personales, mismos que son obligatorios y exigibles al interior de la organización del responsable, además de destinar los recursos necesarios para la implementación de dichos programas y políticas.

El programa sienta las bases para el establecimiento de un sistema de gestión que permite proveer los elementos y actividades de dirección, operación y control de los procesos de la organización, para proteger, de manera sistemática y continua, los datos personales que estén en posesión del Insus.

Conforme a las recomendaciones del Inai, en materia de seguridad de datos personales, fue que se organizó el Sistema de Seguridad de Datos Personales del Insus, mismo que consta de las siguientes fases:

	Fase	Actividad
Proceso	Planear	Identificar políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por el Instituto o sus encargados.
	Hacer	Implementar y operar las políticas, objetivos, planes, procesos, y procedimientos establecidos en la fase anterior.
	Verificar	Evaluar y medir los resultados de lo implementado, a fin de verificar el adecuado funcionamiento del sistema de gestión y el logro de la mejora esperada.
	Actuar	Adoptar medidas correctivas y preventivas en función de los resultados y de la revisión





		realizada, o de otra información relevante, para lograr la mejora continua.
--	--	---

Marco normativo

Constitución Política de los Estados Unidos Mexicanos.

El derecho humano a la protección de los datos personales está previsto en los artículos 6, apartado A, fracciones II, y III, y 16, segundo párrafo, mismos que reconocen que la información relativa a la vida privada y a los datos personales será protegida, en los términos que fijen las leyes de la materia. Además de señalar que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de éstos, así como a manifestar su oposición al uso de su información personal, los llamados derechos ARCO.

De igual manera, los ordenamientos normativos de la materia establecerán los supuestos de excepción a los principios que rijan el tratamiento de datos personales, como lo pueden ser razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas, o para proteger los derechos de terceros.

Ley General de Transparencia y Acceso a la Información Pública.

En términos del artículo 68 de esta ley, son responsabilidades de los sujetos obligados, con respecto a los datos personales en su posesión, la adopción de procedimientos para recibir y responder las solicitudes de derechos ARCO, así como capacitar a las persona servidoras públicas, tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos, en relación con los propósitos para los cuales se hayan obtenido; poner a disposición de los individuos el documento en el que se establezcan los propósitos para su tratamiento en el momento en el cual se recaben datos personales, y adoptar las medidas necesarias que garanticen la seguridad de los datos personales.

Además, la citada norma establece que los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso de los individuos, por escrito o por un medio de autenticación similar.



Ley General de Datos Personales en Posesión de los Sujetos Obligados.

Esta ley establece las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales, y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos. De igual manera, garantiza la observancia de los principios de protección de datos personales, de los cuales destaca el principio de responsabilidad, el cual exige a los responsables y encargados del tratamiento de datos personales, adoptar medidas apropiadas para cumplir con las obligaciones legales, así como estar en capacidad de evidenciar el correcto cumplimiento de sus deberes. En ese sentido, deberán contar con mecanismos idóneos que les permitan probar lo anterior ante las autoridades y los titulares de los datos.

De igual manera, resulta relevante lo dispuesto en el artículo 30 del ordenamiento en cuestión, el cual señala los mecanismos en materia de protección de datos personales que debe implementar el responsable, tales como: elaborar políticas y programas en materia de protección de datos personales; destinar recursos para su instrumentación, además de realizar una revisión periódica, así como poner en práctica un programa de capacitación del personal; establecer procedimientos para recibir dudas y quejas de los titulares; garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, que implique el tratamiento de datos personales, cumplan con las obligaciones previstas en la presente ley.

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

Tienen por objeto desarrollar las disposiciones previstas en la Ley General de Protección Datos Personales. Asimismo, en su artículo 47 precisa que 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.

Estatuto Orgánico del Instituto Nacional del Suelo Sustentable.



2024
AÑO DE
Felipe Carrillo
PUERTO
RENERGIDO DEL PROLETARIADO,
REVOLUCIONARIO Y DEFENSOR
DEL MAÍZ



Establece las bases generales para la organización del Insus.

Glosario

Aviso de Privacidad: Documento a disposición de la persona titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos.

Consentimiento: Manifestación de la voluntad libre, específica e informada de la persona titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

Datos personales: Cualquier información que sea concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse, directa o indirectamente, a través de cualquier información.

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

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.

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

Insus: Instituto Nacional del Suelo Sustentable, en su calidad de responsable del tratamiento de los datos personales que se encuentran en su posesión.



Ley: 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: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

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.

Persona titular: La persona física a quien corresponden los datos personales.

Programa: Programa de Protección de Datos Personales del Instituto Nacional del Suelo Sustentable.

Sistema de Gestión: El Sistema de Gestión de Seguridad de Datos Personales que, de conformidad con el artículo 34 de la Ley, es un conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, así como el cumplimiento de los principios, deberes y obligaciones previstos en dicha ley y las demás disposiciones que resulten aplicables en la materia.





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.



Principios del Tratamiento de Datos Personales

Principio de licitud. Los datos personales tienen que ser tratados de manera lícita, esto es, que el tratamiento debe sujetarse a las facultades o atribuciones que la normatividad aplicable otorga al Instituto.

Principio de lealtad. La obtención de los datos personales no podrá hacerse a través de medios engañosos, ni fraudulentos.

Principio del consentimiento. Como regla general, las áreas que realicen tratamiento de datos personales deberán contar con el consentimiento del titular para el tratamiento de sus datos personales, el cual deberá ir siempre ligado a las finalidades concretas del tratamiento que se informen en el aviso de privacidad.

Principio de información. Las unidades administrativas del Insus que realizan tratamientos de datos personales se encuentran obligadas a informar las personas titulares de los datos, las características principales del tratamiento al que serán sometidos sus datos personales, a través de los avisos de privacidad integral y simplificado,, a fin de que pueda tomar decisiones informadas al respecto.

Principio de proporcionalidad. Las unidades administrativas que realicen tratamiento de datos personales deberán tratar solo aquellos datos personales que resulten necesarios, adecuados y relevantes, en relación con las finalidades para las cuales se obtuvieron.

Principio de finalidad. Los datos personales sólo pueden ser tratados para cumplir con la finalidad, o finalidades, que hayan sido informadas a la persona titular en el aviso de privacidad y, en su caso, consentidas por ésta. Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales.

Principio de calidad. El principio de calidad significa que, conforme a la finalidad, o finalidades del tratamiento que se le vaya a dar los datos personales, éstos deben cumplir las siguientes características:

- Exactos. Los datos personales son exactos cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles.
- Completos. Los datos personales están completos cuando no falta ninguno de los que se requiera para las finalidades para las cuales



se obtuvieron, y son tratados de forma tal que no se cause un daño o perjuicio a su titular.

- **Pertinentes.** Los datos personales son pertinentes cuando corresponden efectivamente a su titular.
- **Actualizados.** Los datos están actualizados cuando están al día y corresponden a la situación real de su titular.
- **Correctos.** Los datos personales son correctos cuando cumplen con todas las características anteriores.

Principio de responsabilidad. A este principio se le conoce también como el principio de “rendición de cuentas”, ya que establece la obligación de los responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y a la autoridad, que cumple con sus obligaciones en torno a la protección de los datos personales.

Deber de confidencialidad. Este deber implica la obligación de guardar secreto respecto de los datos personales que son tratados. Este deber debe cumplirse para evitar causar un daño a su titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información.

Deber de seguridad. Este deber se refiere a la obligación de establecer y mantener medidas de seguridad, tanto técnicas como físicas y administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.



Objetivo General del Programa

Determinar el marco normativo interno para los procesos del ejercicio 2024, en materia de protección de los datos personales en posesión del Insus.

Objetivos específicos del Programa

1. Establecer el proceso de seguimiento al cumplimiento de las obligaciones que establece la Ley y los Lineamientos Generales, así como las demás disposiciones aplicables en materia de protección de datos personales.
2. 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.
3. Promover la adopción de mejores prácticas en la protección de datos personales, de manera preferente, una vez que el programa se haya implementado de manera integral en el Insus, o bien, cuando se estime pertinente la implementación de buenas prácticas.

Responsables de la implementación del Programa

1. Comité de Transparencia

Con fundamento en lo dispuesto por los artículos 83 y, 84, fracción I de la Ley, y 47, segundo párrafo, así como 48 de los Lineamientos, mismos que señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales, y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano colegiado tendrá las siguientes funciones con relación a este programa:

- I. Aprobar, coordinar y supervisar el Programa, en coordinación con las unidades que estime necesario involucrar o consultar;



- II. Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;
- III. Dar a conocer el Programa al interior del Insus;
- IV. Coordinar la implementación del Programa en el Insus;
- V. Con el apoyo de la Unidad de Transparencia, sesorar a las áreas del Insus en la implementación de este Programa.
- VI. Presentar un informe anual en el que se describan las acciones realizadas para cumplir con lo dispuesto por este Programa;
- VII. Supervisar la correcta implementación del Programa;
- VIII. Aprobar, coordinar y supervisar el Programa Anual de Capacitación, en coordinación con las áreas técnicas que se estime necesario involucrar o consultar, y
- IX. Las demás que de manera expresa señale el propio Programa.

El informe al que refiere la fracción VI, deberá presentarse en las primeras dos semanas del mes de marzo de cada año, y se referirá al año inmediato anterior. Algunos de los elementos que pueden incluirse en el informe son:

1. Estadística e información general sobre el cumplimiento de las obligaciones señaladas en el Programa, por parte de las unidades administrativas del Insus;
2. Acciones realizadas por el Comité y la Unidad de Transparencia para cumplir con los objetivos que establece el Programa, y
3. Los resultados de las revisiones y/o auditorías que se realicen en la materia.

○ **Unidad de Transparencia (UT):**

El Artículo 85 de la Ley establece que la Unidad de Transparencia tendrá las siguientes funciones:

- I. Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales;
- II. Gestionar las solicitudes para el ejercicio de los derechos ARCO;
- III. Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados;
- IV. Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables;



- V. Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
- VI. Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO.
- VII. Asesorar a las áreas adscritas al responsable en materia de protección de datos personales
- VIII. Elaborar y proponer al Comité de Transparencia las políticas y programas de protección de datos personales obligatorios y exigibles al interior del Insus, así como fungir dentro del mismo como órgano de consulta en la materia.
- IX. Asesorar a las unidades administrativas del Insus en la implementación de este Programa.



Alcance del Programa.

El Programa será aplicable a todas las unidades administrativas del Insus que realicen tratamiento de datos personales en ejercicio de sus atribuciones. Las unidades administrativas del Instituto Nacional del Suelo Sustentable, de acuerdo con el Estatuto Orgánico, que deberán observar el Programa son las siguientes:

- a) Dirección General.
- b) Dirección de Planeación y Evaluación de Proyectos.
- c) Dirección de Asuntos Jurídicos.
- d) Dirección de Gestión del Suelo.
- e) Dirección de Regularización.
- f) Dirección de Administración y Finanzas.
- g) Representación Regional en Sonora, Baja California y Chihuahua.
- h) Representación Regional en Coahuila y Zacatecas.
- i) Representación Regional en Sinaloa, Durango y Baja California Sur.
- j) Representación Regional en Nuevo León, Tamaulipas y San Luis Potosí.
- k) Representación Regional en Jalisco, Nayarit, Colima y Michoacán.
- l) Representación Regional en Querétaro, Guanajuato y Aguascalientes.
- m) Representación Regional en Ciudad de México, Estado de México, Hidalgo y Morelos.
- n) Representación Regional en Puebla, Guerrero, Tlaxcala y Oaxaca.
- o) Representación Regional en Veracruz, Tabasco y Chiapas.
- p) Representación Regional en Quintana Roo, Campeche y Yucatán.
- q) Oficina de Representación en el Instituto Nacional del Suelo Sustentable



Identificación y Categorización de Datos Personales

- **Datos ideológicos.** Información sobre las posturas ideológicas, religiosas, filosóficas o morales de una persona.
- **Datos sobre opiniones políticas.** Opinión de una persona con relación a un hecho político, o sobre su postura política en general.
Datos sobre afiliación sindical. Pertenencia de una persona a un sindicato y la información que de ello derive.
- **Datos de salud.** Información concerniente a una persona física relacionada con la valoración, preservación, cuidado, mejoramiento y recuperación de su estado de salud físico o mental, presente, pasado o futuro, así como información genética.
- **Datos sobre vida sexual.** Información de una persona física relacionada con su comportamiento, preferencias, prácticas o hábitos sexuales, entre otros.
- **Datos de origen étnico o racial.** Información concerniente a una persona física relativa a su pertenencia a un pueblo, etnia o región que la distingue por sus condiciones e identidades sociales, culturales y económicas, así como por sus costumbres, tradiciones, creencias.



Ciclo de vida de los Datos Personales





Responsables del Tratamiento de Datos Personales

Unidad administrativa	Descripción de la función en la que interviene el tratamiento de datos personales
Coordinación Técnica	<p>Atiende las solicitudes de acceso a la información y de datos personales., además de llevar a cabo el tratamiento de datos personales, y da cumplimiento a lo mandatado por la Ley en la materia.</p> <p>Asimismo, atiende las observaciones y recomendaciones emitidas por los órganos competentes en materia de derechos humanos.</p>
Coordinación Operativa de Representaciones Regionales	<p>Verifica y confirma la identidad del titular de los datos personales, así como la autenticidad de la información que proporciona para contar con un registro que permita identificar con precisión, quién solicita el trámite o servicio ante esta entidad.</p> <p>Asimismo, utiliza los datos personales que proporciona el titular (de los datos personales) para cumplir con los requisitos establecidos en las reglas de operación de los programas sociales, a cargo de este Instituto, y estar en posibilidad de proveerle el apoyo que otorgan los programas presupuestarios, si resulta beneficiado.</p> <p>Finalmente, registra los datos personales del titular con la finalidad de llevar a cabo trámites administrativos, relacionados con peticiones de la ciudadanía.</p>
Dirección de Planeación y Evaluación de Proyectos	<p>Verificar y confirmar la identidad del titular de los datos personales, así como la autenticidad de la información que proporciona para contar con un registro que permita identificar con precisión, quién solicita el trámite o servicio ante esta entidad.</p>





	<p>Cumplir con los requisitos establecidos en las Reglas de Operación de los programas a cargo de este Instituto.</p> <p>Proveer el apoyo solicitado al interesado si resulta beneficiado.</p> <p>Realizar trámites administrativos relacionados con los expedientes, entre otros.</p>
Dirección de Asuntos Jurídicos	<p>Verificar y confirmar la identidad del titular de los datos personales, así como la autenticidad de la información que proporciona para contar con un registro que permita identificar con precisión, quién solicita el trámite o servicio ante esta entidad.</p> <p>Además, utiliza y revisa que los datos personales que proporciona el titular cumplan con los requisitos establecidos en la normatividad vigente que nos rige, y se puedan llevar a cabo los trámites administrativos ante este Instituto.</p>
Dirección de Gestión del Suelo	<p>Verificar y confirmar la identidad del titular de los datos personales, así como la autenticidad de la información que proporciona para contar con un registro que permita identificar con precisión, quién solicita el trámite o servicio ante esta entidad.</p> <p>Utiliza los datos personales que proporciona el titular para cumplir con los requisitos establecidos en las reglas de operación de los programas a cargo de este Instituto, a fin de llevar a cabo los trámites administrativos relacionados con los expedientes o de cartera vencida.</p>
Dirección de Administración y Finanzas	<p>Integra el expediente único de personal, así como los tramites de contratación, nombramiento e identificación, alta y baja y movimientos del personal; otorgamiento de prestaciones de seguridad social, económicas y de salud, además del registro de asistencia digital, pago de remuneraciones, alta y registro</p>





	de los trabajadores y sus beneficiarios del seguro de vida institucional.
Representación Regional en Sonora, Baja California y Chihuahua.	<p>Acredita la personalidad con la que comparece el titular, y recibe su solicitud de regularización. Adicionalmente, procesa los datos en los sistemas de información diseñados para tal efecto y suscribe los formatos relacionados con los trámites, dentro del proceso de regularización, y</p> <p>Conformación e integración el padrón de beneficiarios de los programas S213 <i>Programa para Regularizar Asentamientos Humanos</i> y S273 <i>Programa de Mejoramiento Urbanos</i>, respectivamente, en su vertiente de Regularización y certeza jurídica según corresponda.</p>
Representación Regional en Coahuila y Zacatecas.	<p>Acreditar la personalidad con la que comparece el titular de los datos personales; recibir su solicitud de regularización; procesar los datos en los sistemas de información diseñados para tal efecto; suscribir los formatos relacionados con los trámites dentro del proceso de regularización y,</p> <p>Conformación e integración del padrón de beneficiarios, del programa S213 <i>Programa para Regularizar Asentamientos Humanos</i> y S273 <i>Programa de Mejoramiento Urbanos</i>, en su vertiente de Regularización y certeza jurídica según corresponda.</p>
Representación Regional en Nuevo León, Tamaulipas y San Luis Potosí.	<p>Acreditar la personalidad con la que comparece el titular;</p> <p>Recibir su solicitud de regularización;</p> <p>Procesar los datos en los sistemas de información diseñados para tal efecto;</p> <p>Suscribir los formatos relacionados con los trámites dentro del proceso de regularización y,</p> <p>Conformación e integración del padrón de beneficiarios, del programa S213 <i>Programa para Regularizar Asentamientos Humanos</i> y S273 <i>Programa de Mejoramiento Urbanos</i>, en su vertiente de Regularización y certeza jurídica según corresponda.</p>





Representación Regional en Sinaloa, Durango y Baja California Sur.	<p>Acreditar la personalidad con la que comparece el titular;</p> <p>Recibir su solicitud de regularización;</p> <p>Procesar los datos en los sistemas de información diseñados para tal efecto;</p> <p>Suscribir los formatos relacionados con los trámites dentro del proceso de regularización y, Conformación e integración del padrón de beneficiarios, del programa <i>S213 Programa para Regularizar Asentamientos Humanos</i> y <i>S273 Programa de Mejoramiento Urbanos</i>, en su vertiente de Regularización y certeza jurídica según corresponda.</p>
Representación Regional en Jalisco, Nayarit, Colima y Michoacán.	<p>Acreditar la personalidad con la que comparece el titular;</p> <p>Recibir su solicitud de regularización;</p> <p>Procesar los datos en los sistemas de información diseñados para tal efecto;</p> <p>Suscribir los formatos relacionados con los trámites dentro del proceso de regularización y, Conformación e integración del padrón de beneficiarios, del programa <i>S213 Programa para Regularizar Asentamientos Humanos</i> y <i>S273 Programa de Mejoramiento Urbanos</i>, en su vertiente de Regularización y certeza jurídica según corresponda.</p>
Representación Regional en Querétaro, Guanajuato y Aguascalientes.	<p>Acreditar la personalidad con la que comparece el titular;</p> <p>Recibir su solicitud de regularización;</p> <p>Procesar los datos en los sistemas de información diseñados para tal efecto;</p> <p>Suscribir los formatos relacionados con los trámites dentro del proceso de regularización y, Conformación e integración del padrón de beneficiarios, del programa <i>S213 Programa para Regularizar Asentamientos Humanos</i> y <i>S273 Programa de Mejoramiento Urbanos</i>, en su vertiente de Regularización y certeza jurídica según corresponda.</p>
Representación Regional en Ciudad de México, Hidalgo, Morelos y el estado de México.	<p>Acreditar la personalidad con la que comparece el titular;</p> <p>Recibir su solicitud de regularización;</p> <p>Procesar los datos en los sistemas de información diseñados para tal efecto;</p>





	Suscribir los formatos relacionados con los trámites dentro del proceso de regularización y, Conformación e integración del padrón de beneficiarios, del programa S213 <i>Programa para Regularizar Asentamientos Humanos</i> y S273 <i>Programa de Mejoramiento Urbanos</i> , en su vertiente de Regularización y certeza jurídica según corresponda.
Representación Regional en Veracruz, Tabasco y Chiapas.	Acreditar la personalidad con la que comparece el titular; Recibir su solicitud de regularización; Procesar los datos en los sistemas de información diseñados para tal efecto; Suscribir los formatos relacionados con los trámites dentro del proceso de regularización y, Conformación e integración del padrón de beneficiarios, del programa S213 <i>Programa para Regularizar Asentamientos Humanos</i> y S273 <i>Programa de Mejoramiento Urbanos</i> , en su vertiente de Regularización y certeza jurídica según corresponda.
Representación Regional en Puebla, Guerrero, Tlaxcala y Oaxaca.	Acreditar la personalidad con la que comparece el titular; Recibir su solicitud de regularización; Procesar los datos en los sistemas de información diseñados para tal efecto; Suscribir los formatos relacionados con los trámites dentro del proceso de regularización y, Conformación e integración del padrón de beneficiarios, del programa S213 <i>Programa para Regularizar Asentamientos Humanos</i> y S273 <i>Programa de Mejoramiento Urbanos</i> , en su vertiente de Regularización y certeza jurídica según corresponda.
Representación Regional en Quintana Roo, Campeche y Yucatán.	Acreditar la personalidad con la que comparece el titular; Recibir su solicitud de regularización; Procesar los datos en los sistemas de información diseñados para tal efecto; Suscribir los formatos relacionados con los trámites dentro del proceso de regularización y, Conformación e integración del padrón de beneficiarios, del programa S213 <i>Programa para Regularizar Asentamientos Humanos</i> y S273





	<p><i>Programa de Mejoramiento Urbanos</i>, en su vertiente de Regularización y certeza jurídica según corresponda.</p>
<p>Oficina de Representación en el Instituto Nacional del Suelo Sustentable</p>	<p>La elaboración de informes de irregularidades detectadas por presuntas faltas administrativas.</p> <p>La atención de las quejas o denuncias que presenten las personas físicas o morales, por actos u omisiones cometidos por personas servidoras públicas dependientes jerárquica y funcionalmente de este Instituto, o de particulares por conductas sancionables en términos de la Ley General de Responsabilidades Administrativas-</p> <p>Integración de los expedientes para la substanciación y, en su caso, resolución de Procedimientos de responsabilidades Administrativas.</p> <p>Notificación a las personas servidoras públicas de las constancias del expediente de presuntas responsabilidades administrativas integrado en la investigación, así como de las demás constancias y pruebas que hayan aportado u ofrecido las autoridades investigadoras para sustentar dicho Informe.</p> <p>Remitir las constancias originales del expediente del procedimiento de responsabilidad administrativa al Tribunal encargado de resolver el asunto, así como cualquier procedimiento administrativo que el Órgano Interno de Control realice de acuerdo con el Reglamento Interior de la Secretaría de la Función Pública.</p> <p>Para la participación en los procesos de Entrega Recepción y de Rendición de Cuentas de las personas servidoras públicas del Instituto.</p> <p>Para el control de los números de oficio que se designan para tratar los diversos temas del Órgano Interno de Control.</p>





	<p>Ingresar información que se desprenda para la continuidad en las denuncias dentro del Sistema Integral de Denuncias Ciudadanas. (SIDECE).</p> <p>Incorporar, identificar y localizar información para seguimiento de los procedimientos de responsabilidad administrativa en el Sistema Integral de Responsabilidades Administrativas (SIRA).</p> <p>Consultar de forma histórica la información contenida en el Sistema de Procedimientos Administrativos de Responsabilidades. (SPAR).</p> <p>Incorporar, identificar y localizar información para el seguimiento de los procedimientos administrativos de inconformidad en el Sistema Integral de Inconformidades (SIINC), y en los expedientes de investigación en el Sistema de Procedimiento Administrativo de Sanciones a Proveedores y Contratistas (SANC).</p>
--	--

Estrategias y acciones

Las estrategias contenidas en el presente Programa de Protección de Datos Personales del Insus, se encuentran alineadas a la normativa Institucional, las cuales serán desarrolladas bajo la coordinación de la Unidad de Transparencia, y la tutela del Comité de Transparencia de la Institución. Dichas estrategias fueron diseñadas, a partir del análisis de la problemática que enfrenta la institución en el Tratamiento de Datos Personales, así como del análisis de los posibles mecanismos para el correcto tratamiento de dichos datos personales.

En este sentido, las estrategias del presente Programa son:

Estrategias	Definición
1. Sensibilización	Capacitación y acompañamiento en materia de protección de datos personales.



2. Seguimiento	Actualización de documentos para el tratamiento de datos personales.
----------------	--

De las estrategias, se derivan las siguientes actividades:

Estrategia	Acciones
1. Sensibilización	1.1. Gestionar las acciones de capacitación en materia de datos personales para las personas servidoras públicas del Insus. 1.2. Proporcionar acompañamiento para la elaboración de instrumentos o productos derivados de la normatividad en materia de protección de datos personales. 3. Difundir en las unidades administrativas formatos, instructivos, guías o marcos de referencia, proporcionados por el Inai, que sirvan de apoyo en el cumplimiento de obligaciones y deberes de protección de datos personales. 4. Difundir en las unidades administrativas la normatividad en materia de protección de datos personales, así como, en su caso, materiales de apoyo relacionados con la misma.

Estrategia	Acciones
2. Seguimiento	2.1. Revisión y, en su caso, actualización de la documentación referente a la protección de datos personales del Insus.

Mejora continua

Se adoptarán las medidas preventivas y correctivas que hayan resultado de las verificaciones, revisiones y auditorías realizadas por el Inai 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:



Acciones preventivas: Son aquellas encaminadas a evitar cualquier vulneración con relación a lo establecido en este programa, y se deben llevar a cabo las siguientes actividades:

- Analizar y revisar de las posibles causas de una vulneración;
- Determinar las vulneraciones que podría desencadenarse, a partir de ciertas situaciones de riesgo, en el tratamiento de datos personales;
- Evaluar las acciones necesarias para evitar que ocurra una vulneración;
- Documentar los resultados de las acciones tomadas, y
- Revisar la eficacia de las acciones preventivas tomadas.

1. **Acciones correctivas:** Son aquellas encaminadas a eliminar las causas de que generan las vulneraciones, con relación a lo previsto en este programa, y se deben llevar a cabo, al menos, las siguientes actividades:

- Analizar y revisar las vulneraciones;
- Determinar las causas que dieron origen a la vulneración;
- Evaluar las acciones necesarias para evitar que la vulneración vuelva a ocurrir;
- Informar sin dilación al titular de los datos personales para que éste pueda tomar las medidas correspondientes para la protección de sus derechos, así mismo se deberá informar al órgano garante. El servidor público que vulnere el derecho de protección de datos personales deberá acreditar dos cursos de protección de datos personales por año.
- Documentar los resultados de las acciones tomadas, y
- Revisar la eficacia de las acciones correctivas tomadas.

De igual manera, el Comité de Transparencia deberá establecer un plazo límite para que se corrijan las vulneraciones detectadas, y documentar las medidas preventivas o correctivas realizadas para la mejora continua en la implementación de este Programa.



Respuesta a incidentes o vulneraciones de seguridad

Se considerarán como vulneraciones de seguridad, en cualquier fase del Tratamiento de datos personales, las siguientes:

- Pérdida o destrucción, parcial o total, no autorizada de datos personales.
- Robo, extravío o copia no autorizada de datos personales.
- Uso, acceso o tratamiento no autorizado
- Daño, alteración o modificación, parcial o total, no autorizada

Por otro lado, la notificación de vulneraciones de seguridad se llevará a cabo con el objeto de dar cabal cumplimiento a lo previsto en el artículo 40 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), que establece la obligación a cargo del Insus de informar sin dilación alguna a la persona titular, y según corresponda, al Inai. Las vulneraciones que afecten de forma significativa (énfasis añadido), los derechos patrimoniales o morales, se deberán notificar 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. El plazo de 72 horas comenzará a correr el mismo día natural en que el responsable confirme la vulneración de seguridad.

El procedimiento para llevar a cabo la notificación de vulneraciones de seguridad se realizará a través de un formato de notificación, en donde se incluya la descripción de la siguiente información:

1. La naturaleza del incidente o vulneración ocurrida;
2. Los datos personales comprometidos;
3. Las recomendaciones al titular de los datos personales acerca de las medidas que éste deba adoptar para proteger sus intereses;
4. Las acciones correctivas realizadas de forma inmediata;
5. Los medios en donde puede obtener más información al respecto;
6. La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular de los datos personales a entender el impacto del incidente y,



7. Cualquier otra información y documentación que considere conveniente para apoyar a los titulares de datos personales.

De igual manera, se deberá actualizar la bitácora o registro de las vulneraciones a la seguridad de los datos personales, en la que se tendrán que describir dichas vulneraciones, la fecha en la que ocurrieron, el motivo de éstas y las acciones correctivas que se llevaron a cabo.

Sanciones

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

De manera adicional, es importante que las personas servidoras públicas que están a cargo del tratamiento de datos personales tengan presente que de conformidad con el artículo 163 de la Ley General de Datos Personales serán causas de sanción, por incumplimiento de las obligaciones establecidas en dicha ley, las siguientes:

- I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;
- II. Incumplir los plazos de atención previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados para responder las solicitudes para el ejercicio de los derechos ARCO, o para hacer efectivo el derecho de que se trate;
- III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida, datos personales que se encuentren bajo su custodia, o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
- IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la Ley General de Datos Personales;
- V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la Ley



- General de Datos Personales, según sea el caso, y demás disposiciones que resulten aplicables en la materia;
- VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;
 - VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la Ley General de Datos Personales;
 - VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la Ley General de Datos Personales;
 - IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la Ley General de Datos Personales;
 - X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en Ley General de Datos Personales;
 - IX. Obstruir los actos de verificación de la autoridad;
 - X. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la Ley General de Datos Personales;
 - XI. No acatar las resoluciones emitidas por el Instituto, y
 - XII. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia, o bien, entregar el mismo de manera extemporánea. Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves. Asimismo, de conformidad con el artículo 105 de los Lineamientos Generales, cuando alguna unidad administrativa se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, ésta dará aviso al superior jerárquico para que le ordene realizar sin demora las acciones conducentes. Si persiste la negativa de colaboración, la Unidad de Transparencia lo hará del conocimiento del Comité de Transparencia para que, a su vez, dé vista al Órgano Interno de Control, contraloría o instancia equivalente y, en su caso, dé inicio el procedimiento de responsabilidad administrativo respectivo de conformidad con la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos. Cabe destacar que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

