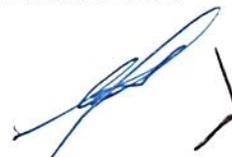


Programa de Protección de Datos Personales de la SEDATU 2021

Fecha de autorización: Junio 2021.





Índice

Presentación:..... 4

Introducción:..... 5

Marco Normativo:..... 6

Alcance:..... 7

Objetivos:..... 8

Principios y deberes en el tratamiento de datos personales:..... 8

Ejes Problemáticos:..... 12

 1) Cultura para la protección de los datos personales dentro de la SEDATU..... 12

 2) Capacitación en materia de Protección de datos personales 12

 3) Ejercicio de los derechos ARCO 12

 4) Implementación, seguimiento y actualización de los mecanismos y/o documentos que dan certeza al deber de Protección de Datos Personales. 14

 5) Acciones preventivas en materia de protección de datos personales. 14

Líneas estratégicas:..... 15

 1) Sensibilización y capacitación sobre la protección de los datos personales..... 15

 2) Fortalecimiento Institucional..... 16

 3) Implementación, revisión y mejora de las acciones diseñadas para el tratamiento y seguridad de los Datos Personales. 17

Mejora del Programa de Protección de Datos Personales:..... 18

 DIRECTORIO 19





Glosario/Definiciones:

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.

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

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. Por ejemplo aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición 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.

Líneas estratégicas: El conjunto de líneas de acción interrelacionadas que permiten organizar la atención que brinda la estrategia a la problemática para la consecución del objetivo.

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

Objetivo: El fin general al que se ajusta el programa y que se asocia unívocamente con las estrategias.

Ejes problemáticos: Asuntos que implican algún tipo de inconveniente o trastorno y que exigen una solución.

Responsable: Los sujetos obligados a que se refiere el artículo 1 de la LGPDPSO que deciden sobre el tratamiento de datos personales.

Titular: La persona física a quien corresponden los datos personales.

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: Área a la que se le confiere atribuciones específicas en el reglamento interno, estatuto orgánico o instrumento normativo equivalente que sea superior a un manual de organización.

Presentación:

Debido al aumento de las tecnologías de la información y las comunicaciones, se ha redimensionado las relaciones del ser humano e incrementado los procesos de comunicación de la sociedad globalizada, provocando que hoy en día, el manejo e intenso intercambio de la información se haya convertido en la columna vertebral de las actividades cotidianas que realizan las personas, instituciones públicas y/o empresas.

En este sentido, el tratamiento que se le da a los datos personales, se ha convertido en una práctica tan necesaria como habitual de control y almacenamiento por parte de los sectores tanto públicos como privados.

Por lo que, el tema de la protección de datos personales toma relevancia cada vez mayor tanto en el mundo como en nuestro País, pero sobre todo representa un reto importante mantener segura la información que contenga datos personales de las y los titulares de los mismos.

En nuestro país, el derecho a la **protección de datos personales** se encuentra reconocido en la Constitución Política de los Estados Unidos Mexicanos, como un derecho a favor de la autodeterminación informativa y, desde luego, de la dignidad de la persona humana.

En el sector público encuentra su antecedente en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental publicada en 2002; posteriormente, las reformas en materia de transparencia, acceso a la información y protección de datos personales contempladas en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos en 2009 y 2014, propiciaron la emisión de diversa normatividad con el propósito de garantizar el ejercicio de este derecho humano; entre ellas la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPO), publicada el 26 de enero de 2017 y en la cual se establecen las bases, procedimientos, principios, deberes y obligaciones que rigen el tratamiento de información de carácter personal, así como los derechos que tienen los titulares a la protección de sus datos personales.

Por lo anterior, la tutela y protección de datos personales deben ser asumidas como un deber y a la par como un reto, para evitar cualquier riesgo a la intimidad y privacidad de las personas, frente a los avances tecnológicos que ha traído consigo el uso de los datos personales.

En este marco, la **Secretaría de Desarrollo Agrario, Territorial y Urbano (SEDATU)** en su carácter de Sujeto Obligado reconocido por la LGPDPPSO, tiene la obligación de cumplir con lo dispuesto en el marco normativo aplicable, debiendo respetar los principios, deberes y obligaciones previstos en dicha Ley, entre ellos el de implementar los mecanismos necesarios para proteger los datos personales y cumplir con el principio de responsabilidad.





Introducción:

En atención a que la **SEDATU** es la institución de la Administración Pública Federal que tiene a su cargo entre otras funciones: planificar, coordinar, administrar, generar y ejecutar las políticas públicas de ordenamiento territorial; regular la propiedad social (ejidos, las parcelas, las tierras ejidales y comunales, la pequeña propiedad agrícola, ganadera y forestal, los terrenos baldíos y nacionales); asegurar una vivienda adecuada, un desarrollo urbano y rural así como otorgar certeza jurídica a los núcleos agrarios; buscando mejorar la calidad de la vida de las y los mexicanos, prevenir los asentamientos en zonas de riesgo y coadyuvar en caso de fenómenos naturales para la atención inmediata; y es un sujeto obligado, en materia de protección de datos personales que tiene el deber y la obligación de garantizar la protección de los datos personales, y por ende responsable del tratamiento de dichos datos, para el ejercicio de sus funciones, la Dirección de la Unidad de Enlace con el INAI, de la Dirección General de Legislación, Consulta y Pago de Predios, adscrita a la Unidad de Asuntos Jurídicos, con la participación de las diversas Unidades Administrativas que integran la SEDATU, ha diseñado y elaborado el presente **Programa de Protección de Datos Personales**, como una herramienta de las acciones mínimas que deberán considerarse para la eficaz protección de datos personales recabados en atención a las atribuciones de cada unidad administrativa de la Dependencia.

Su elaboración se llevó a cabo en cumplimiento de lo dispuesto por los **artículos 30, fracción II, de la LGPDPSO, así como 47 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público**; además, se realizó en el marco del **Programa Nacional de Protección de Datos Personales 2018-2022 (PRONADATOS)**, aprobado por acuerdo publicado en el Diario Oficial de la Federación el 26 de enero de 2018.

Cabe mencionar que dicho Programa Nacional, es el principal instrumento que tiene el **Sistema Nacional de Transparencia (SNT)** para definir y coordinar las bases de la política pública de protección de datos personales en el país, dentro del sector público; pues propone acciones en temas como promoción de la cultura de la protección de datos personales, capacitación y medidas de seguridad de la información, y tiene como objetivo primordial fortalecer las instituciones vinculadas con la protección de datos personales para generar un beneficio palpable en la población a través del tratamiento de datos personales en México y como objetivos a corto plazo, busca impulsar el cumplimiento gradual de la LGPDPSO a partir de acciones y estrategias prioritarias, así como identificar los sectores y las áreas relevantes donde la protección de datos personales generará un beneficio y trascendencia pública y social

En este sentido, en este **Programa de Protección de Datos Personales de la SEDATU**, se determinan las pautas generales bajo las cuales se garantizará a los titulares la debida utilización y resguardo de sus datos personales, tratados por las diversas unidades administrativas, en cualquier etapa del ciclo de vida de mismos, es decir, la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición y posterior supresión. Se articula por una serie de actividades interrelacionadas que permitirán implementar, monitorear, revisar y mejorar el tratamiento y seguridad de los datos personales en posesión de la SEDATU, teniendo como ejes la observancia de los principios y deberes previstos en la normatividad de la materia para garantizar la seguridad y tratamiento eficaz de los datos personales, así como maximizar el ejercicio de los derechos ARCO.

Av. Heroica Escuela Naval Militar Número 701, Colonia Presidentes Ejidales Segunda Sección, Coyoacán, C.P.04470. Tel: 55 5209700
www.gob.mx/sedatu





La estructura del presente programa, comprende 5 ejes problemáticos donde se incluye la problemática detectada entorno a ellos; además las 3 líneas estratégicas y de acción previstas para alcanzar los objetivos.

Asimismo, debe indicarse que el presente Programa, ha sido integrado bajo la perspectiva de mantener la continuidad de las acciones implementadas en este año, orientadas a fortalecer la cultura de la protección de datos personales al interior de la propia Secretaría y a monitorear el adecuado cumplimiento de deberes y obligaciones, de forma tal que, la SEDATU en su calidad de responsable, disponga de las medidas seguridad y los protocolos adecuados para la protección de los datos personales que son tratados con motivo del ejercicio de sus funciones, además de maximizar en todo momento el ejercicio de los derechos ARCO ante la dependencia; de ahí que el Programa tenga vigencia multianual (2021-2024).

Marco Normativo:

El derecho a la protección de datos personales, materia de este programa, tiene su fundamento en el marco jurídico siguiente:

- Constitución Política de los Estados Unidos Mexicanos: En el artículo 6º, apartado A, fracción II, se establece que la información relativa a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes; asimismo, el párrafo segundo de su artículo 16 refiere que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley.
- Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108): Fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. Tiene como fin garantizar a cualquier persona física el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.
- Ley General de Transparencia y Acceso a la Información Pública: Tiene por objeto establecer los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier autoridad.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados: Primer ordenamiento mexicano que, a nivel nacional, fija las bases para el efectivo ejercicio y tutela del derecho fundamental a la protección de datos personales dentro del ámbito público, que tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona física a la protección de sus datos personales en posesión de todo ente público.
- Lineamientos Generales de Protección de Datos Personales en Sector Público: Tienen por objeto desarrollar las disposiciones previstas en la LGPDPSO y en específico el artículo 47 determina que el responsable del tratamiento de datos personales deberá elaborar e implementar políticas y programas de protección de datos personales.



- Ley Orgánica de la Administración Pública Federal: Establece las bases de organización de la Administración Pública Federal, centralizada y paraestatal; en el artículo 41 se establecen las atribuciones de la SEDATU.
- Reglamento Interior de la Secretaría de Desarrollo Agrario, Territorial y Urbano: El cual tiene como objetivo, establecer las atribuciones de las áreas que conforman la SEDATU.

Alcance:

El presente Programa de Protección de Datos Personales será aplicable a todas las unidades administrativas de la **Secretaría de Desarrollo Agrario, Territorial y Urbano**, que realicen cualquier tipo de tratamiento de datos personales en ejercicio de sus atribuciones, con excepción de los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que refieren los artículos 120 de la Ley General de Transparencia y Acceso a la Información Pública y 117 de la Ley Federal de Transparencia y Acceso a la Información Pública, disposiciones que prevén las excepciones en las que los responsables podrán permitir el acceso a información confidencial sin requerir el consentimiento del titular, a saber, cuando: la información se encuentre en registros públicos; por ley tenga el carácter de pública; exista una orden judicial; por razones de seguridad nacional, salubridad, para proteger los derechos de terceros o cuando se transmita entre sujetos obligados y entre éstos y los sujetos de derecho internacional, siempre que la información se utilice para el ejercicio de facultades.

Por lo que, en atención al Reglamento Interior de la Dependencia, es de aplicación a las siguientes Unidades administrativas:

- I. Subsecretaría de Ordenamiento Territorial y Agrario, y
- II. Subsecretaría de Desarrollo Urbano y Vivienda;
- III. Unidades y Coordinaciones Generales;
 - a) Unidad de Administración y Finanzas;
 - b) Unidad de Asuntos Jurídicos;
 - c) Unidad de Planeación y Desarrollo Institucional;
 - d) Unidad de Proyectos Estratégicos para el Desarrollo Urbano;
 - e) Unidad de Apoyo a Programas de Infraestructura y Espacios Públicos;
 - f) Coordinación General de Desarrollo Metropolitano y Movilidad, e
 - g) Coordinación General de Gestión Integral de Riesgos de Desastres;
- IV. Direcciones Generales:
 - a) De Coordinación de Oficinas de Representación;
 - b) De Ordenamiento de la Propiedad Rural;
 - c) De Ordenamiento Territorial;
 - d) De Inventarios y Modernización Registral y Catastral;
 - e) De Concertación Agraria y Mediación;
 - f) De Desarrollo Regional;
 - g) De Desarrollo Urbano, Suelo y Vivienda;
 - h) De Programación y Presupuesto;
 - i) De Capital Humano y Desarrollo Organizacional;
 - j) De Recursos Materiales y Servicios Generales;
 - k) De Tecnologías de la Información y Comunicaciones;
 - l) De Amparos y Ejecutorias;





- m) De Litigio Estratégico y Cumplimiento Normativo, e
- n) De Legislación, Consulta y Pago de Predios;

V. Oficinas de Representación en las Entidades Federativas o Regiones.

Cabe mencionar que por ende este Programa aplica a todos las personas servidoras públicas de la SEDATU que por sus funciones realicen algún tipo de tratamiento de datos personales y en este caso, están obligados a conocer y aplicar las medidas de seguridad mínimas, en la LGPDPSO y sus lineamientos Generales.

Objetivos:

El principal objetivo del programa es el de cumplir con el principio de responsabilidad en el tema de la protección de los datos personales, es decir, cumplir con las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales, así como la demás normatividad aplicable y que derive de los mismos.

Posteriormente, con dicho programa establecen directrices y herramientas, para garantizar la protección de los datos personales en posesión de las unidades administrativas de esta Secretaría, por medio de la sensibilización, capacitación, implementación, operación, revisión, mantenimiento y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales, que las Unidades tratan.

Además y como último objetivo, se busca promover la adopción de mejores prácticas en materia de protección de datos personales, a efecto de lograr una mayor participación de la comunidad de la SEDATU con relación al ejercicio de los derechos ARCO, así como brindarle a la ciudadanía la certeza de que sus datos personales en posesión de esta Dependencia están siendo tratados de conformidad con lo establecido en el marco normativo.

Aunado a lo anterior, como objetivo a corto plazo, con este programa se busca fortalecer a la Secretaría de Desarrollo Agrario, Territorial y Urbano, en el tema de protección de datos personales y poder así generar un cambio entre el personal que trata (posee, recaba, almacena, etc.) datos personales en cumplimiento a sus facultades, dentro de la SEDATU.

Por último, no hay que dejar de lado que la comunicación digital, se incrementa día con día y con ello el almacenamiento de los datos resulta un reto importante; por lo que la regulación y sobre todo la guía y/o apoyo, es fundamental para la protección de datos personales.

Principios y deberes en el tratamiento de datos personales:

Todo el personal de la SEDATU que trate datos personales, en cumplimiento de sus funciones, deberá de adoptar las medidas necesarias para evitar que se produzca un riesgo o daño de los mismos, respetando los principios de la protección de datos, mismos que constituyen el pilar mediante el cual se articula este derecho, por lo que son de observancia obligatoria para todo aquél que interviene en el tratamiento de datos personales, mismos que a saber son:





- a) Principio de licitud: Significa que las personas servidoras públicas deberán de asumir un comportamiento ético y responsable, en el tratamiento de los datos personales que poseen en sus unidades administrativas, sujetándose a las atribuciones o facultades que el Reglamento Interior de la Secretaría les confiera.
- b) Principio de lealtad: De acuerdo con este principio, para la obtención de los datos personales las personas servidoras no podrán hacerse a través de medios engañosos, ni fraudulentos, lo que implica que:
- No se recaben datos personales con dolo, mala fe o negligencia;
 - No tratar los datos de tal manera que genere discriminación o un trato injusto contra los titulares.
 - No se vulnere la confianza del titular con relación a que sus datos personales serán tratados conforme a lo acordado; y
 - Se informen todas las finalidades del tratamiento en el aviso de privacidad.
- c) Principio del consentimiento: Como regla general, los sujetos obligados, deberán contar con el consentimiento del titular para el tratamiento de sus datos personales. Para obtener el consentimiento tácito, expreso o expreso por escrito y dependiendo del tipo de datos personales, la solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informen en el aviso de privacidad, es decir, el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas, no en lo general.

Aunado a ello, el consentimiento debe ser informado, por lo que previo a su obtención, es necesario que el titular conozca el aviso de privacidad.

- d) Principio de información: En virtud de este principio, las personas servidoras públicas se encuentran obligadas a informar a los titulares, las características principales del tratamiento al que será sometida su información personal, lo que se materializa a través del aviso de privacidad.

A fin de que los titulares puedan tomar decisiones informadas al respecto y puedan ejercer su derecho a la protección de su información personal. En ese sentido, toda área que trate datos personales, sin importar la actividad que realice, requiere elaborar y poner a disposición los avisos de privacidad que correspondan a los tratamientos que lleven a cabo.

- e) Principio de proporcionalidad: establece la obligación de que las personas responsables, tratarán sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.
- f) Principio de finalidad: Es decir, los datos personales solo pueden ser tratados para cumplir con la finalidad (propósito, motivo o razón por el cual se tratan) o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste.

Las finalidades deben ser:





- **Concretas:** Cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular.
- **Explícitas:** Cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.
- **Lícitas:** Cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación.
- **Legítimas:** Cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General.

Aunado a ello, la finalidad o finalidades del tratamiento de datos personales deberán ser determinadas, es decir, las personas servidoras públicas están obligadas a especificar para qué objeto se tratarán los datos personales de manera clara, sin lugar a confusión y con objetividad; por ejemplo "los datos personales que se le solicitan son para la creación de un expediente laboral, para la atención o seguimiento de un trámite, etc."

- g) Principio de calidad: significa que, conforme a la finalidad o finalidades para las que se vayan a tratar los datos personales, éstos deben ser exactos, correctos, completos y actualizados.

Por lo anterior, los responsables están obligados a:

- Adoptar las medidas que consideren convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, actualizados y correctos, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación;
- Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo;
- Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación de conformidad con lo establecido por la Ley General de Archivos;
- Establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales.

Por lo que será necesario tomar en consideración lo siguiente:

1. La conservación de los datos personales: El plazo de conservación de los datos personales no debe exceder el tiempo estrictamente necesario para llevar a cabo las finalidades que justificaron el tratamiento, ni aquél que se requiera para



cumplir con las disposiciones legales establecidas en la Ley General de Archivos; y las disposiciones aplicables en la materia de que se trate;

2. El bloqueo de los datos personales: Se define como la acción que tiene por objeto impedir el tratamiento de los datos personales para cualquier finalidad, con excepción de su almacenamiento y acceso para determinar posibles responsabilidades en relación con el tratamiento de los datos personales, hasta el plazo de prescripción correspondiente. Por lo que, lo idóneo sería que las personas servidoras bloqueen los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales. Concluido dicho periodo se deberá proceder a su supresión.
- h) Principio de responsabilidad Establece la obligación de las unidades de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y el órgano garante, que cumple con sus obligaciones en torno a la protección de los datos personales.

Finalmente, las unidades administrativas para dar cumplimiento total al marco normativo, en el tema de la protección de los datos personales, además de guiarse y cumplir con los principios y obligaciones, deberán considerar y efectuar dos **deberes** importantes:

- a) Deber de Confidencialidad: Entendiendo por confidencialidad, que se deben de establecer controles o mecanismos que tengan por objeto que todas aquellas personas servidoras y servidores públicos que traten datos personales, en cualquier fase del tratamiento, mantengan en secreto la información, así como evitar que la información sea revelada a personas no autorizadas y prevenir la divulgación no autorizada de la misma.

Es decir, los sujetos responsables, tienen obligación de guardar la debida confidencialidad respecto de los datos personales que son tratados en sus unidades administrativas, para evitar causar un daño a su titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información y hacer mal uso de esta.

- b) Deber de Seguridad: Para una efectiva protección de los datos personales es necesaria la implementación de un Sistema de Gestión de Seguridad de Datos Personales (Sistema de Gestión), que permita planificar, implementar, monitorear y mejorar las medidas de seguridad de carácter administrativo, físico y técnico, a través de una serie de actividades interrelacionadas y documentadas.

En este sentido, las personas servidoras públicas con independencia del tipo de tratamiento que efectúe, deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad de los datos de carácter personal que conozca y a los que tenga acceso durante la relación que mantenga con la Secretaría de Desarrollo Agrario, Territorial y Urbano, debiendo subsistir esta obligación después de finalizar sus relaciones con esta.





Ejes Problemáticos:

1) Cultura para la protección de los datos personales dentro de la SEDATU.

Hoy en día todavía existe desconocimiento sobre el tema de la protección de los datos personales, entre la sociedad y entre el personal adscrito a las Unidades Administrativas de esta Secretaría; por lo que no obstante que la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados se publicó en el Diario Oficial de la Federación el 26 de enero de 2017, su implementación se ha realizado gradualmente, por lo que aún es un tema novedoso.

Asimismo, se ha evidenciado en diversos foros que entre la sociedad hay una gran preocupación de la población sobre el uso de sus datos personales, es decir, la gente desconfía y teme de que cualquier persona pueda localizar su domicilio, o, usen sus números de cuentas bancarias, etc.

Por último, es importante mencionar que las dependencias de gobierno al ser sujetos obligados y responsables del tratamiento de los datos personales, que recaba, almacena y/o utiliza, deben ser reconocidas como dependencias garantes del derecho a la protección de datos personales; en nuestro caso, buscamos que dentro de la SEDATU exista educación y cultura en materia de protección de datos personales, para lograr dicho reconocimiento.

2) Capacitación en materia de Protección de datos personales

Ante el desconocimiento genérico sobre el derecho a la protección de los datos personales y la preocupación de las personas por el mal uso de sus datos personales, los responsables del tratamiento de los datos personales dentro de las Unidades Administrativas deberán estar capacitados y contar con los conocimientos necesarios en el tema; porque si no conocemos las obligaciones y deberes en materia de protección de datos personales, no podemos cumplir con el principio de responsabilidad ni mucho menos con el deber de protección.

Es importante señalar que la capacitación respecto de los alcances del marco normativo en materia de protección de datos personales, así como de la identificación de las buenas prácticas institucionales, permitirán actualizar y sensibilizar al personal de las unidades administrativas, generando una conciencia institucional sobre la trascendencia del tratamiento y la protección de los datos personales que obran en sus bases de datos o documentos institucionales.

3) Ejercicio de los derechos ARCO

La Problemática es que este tema está aún en construcción; fue en 2007 con la reforma al artículo 6° Constitucional, que se reconocieron los derechos que tiene toda persona física de Acceder y Rectificar su información, y fue hasta la reforma del 2009, que se reconoció la protección de datos personales como un derecho fundamental, autónomo y distinto al derecho de acceso a la información; así como el reconocimiento de los derechos de Cancelación y Oposición, garantizando así la totalidad de los derechos ARCO.

En razón de lo anterior, se deben establecer las bases para el ejercicio adecuado de los derechos ARCO (de Acceso, Rectificación, Cancelación y Oposición), mismos que son



reconocidos por la legislación mexicana y que consisten en:

- I. *Derecho de Acceso*: Derecho que tiene el titular de solicitar el acceso a sus datos personales que se encuentran en las bases de datos, sistemas, archivos, registros o expedientes del responsable que los posee, almacena o utiliza.
- II. *Derecho de Rectificación*: Derecho que tiene el titular de solicitar la rectificación o corrección de sus datos personales, cuando éstos sean inexactos o incompletos o no se encuentren actualizados.
- III. *Derecho de Cancelación*: Derecho que tienen los titulares de solicitar que sus datos personales se eliminen de los archivos, registros, expedientes, sistemas, bases de datos del responsable que los trata; aunque no en todos los casos se podrán eliminar sus datos personales, principalmente cuando sean necesarios por alguna cuestión legal o para el cumplimiento de obligaciones.
- IV. *Derecho de Oposición*: Es el derecho que tiene el titular de solicitar que sus datos personales no se utilicen para una determinada finalidad, no para la totalidad de estas. También en este caso, como en el anterior, no siempre se podrá impedir el uso de los datos, cuando estos sean necesarios por motivos legales o para el cumplimiento de obligaciones.

En atención a ello, es que las personas servidoras públicas de la Dependencia, deben tener conocimiento que como cualquier otro derecho, el de protección de datos personales tiene límites, por lo que bajo ciertas circunstancias los derechos ARCO no podrán ejercerse por cuestiones de seguridad nacional; orden, seguridad y salud públicos, así como por derechos de terceros, conforme lo dispone el artículo 6° de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Además, debemos tener muy claro que las únicas causas por las que se puede negar el ejercicio de los derechos ARCO, de acuerdo al artículo 55 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, son:

1. El titular de los datos personales o su representante no hayan acreditado su identidad;
2. El responsable no es competente para atender la solicitud;
3. Existe un impedimento legal;
4. Se pueda afectar los derechos de terceras personas;
5. Cuando el ejercicio de los derechos ARCO pudiera obstaculizar procesos judiciales o administrativos;
6. Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular;
7. Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular;
8. Cuando los datos sean parte de información de las entidades sujetas a regulación y supervisión financiera del sujeto obligado, o
9. Cuando en función de sus atribuciones del sujeto obligado, el uso, resguardo y manejo sean necesarios para mantener la integridad, estabilidad y permanencia del Estado mexicano.





Es por ello que el derecho a la protección de datos personales es un derecho personalísimo, solamente los titulares o sus representantes podrán solicitar el ejercicio de los derechos ARCO.

4) Implementación, seguimiento y actualización de los mecanismos y/o documentos que dan certeza al deber de Protección de Datos Personales.

Podemos englobar que aunado al crecimiento de las nuevas tecnologías y al desconocimiento genérico de la protección de los datos personales, se suma que las medidas de seguridad necesarias para el tratamiento de datos personales carecen de un marco de certeza, creando un desconocimiento tanto de las medidas de seguridad como del tema en general.

En razón de lo anterior y en virtud de que la **SEDATU**, tiene el deber y la obligación de garantizar la protección de los datos personales y el ejercicio de los derechos ARCO, se han creado y adoptado mecanismos para efectuar el cumplimiento de los principios, deberes y obligaciones establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; mismos que se han formalizado en instrumentos o documentos, creados por la Dirección de la Unidad de Enlace con el INAI en coordinación con las diferentes unidades responsables de la Secretaría, que permitirán proteger los datos personales de manera general que se tratan en toda la Dependencia; dichos mecanismos y/o documentos son:

- Políticas de SEDATU para facilitar la obtención de información y el ejercicio del derecho de acceso a la información.
- Las Políticas Internas de Gestión y Tratamiento de Datos Personales, para todas las Unidades de la Secretaría;
- El Documento de Seguridad, el cual describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales, que poseen, utilicen o traten las Unidades Administrativas de la Secretaría;
- El sistema de Gestión de Seguridad de los Datos Personales.

Los cuales se deberán de implementar, pero sobre todo se deberán actualizar y mantener siempre al día, procurando realizar una revisión y mejora periódica.

Cabe mencionar que este Programa de Protección de Datos Personales, forma parte de los mecanismos legales necesarios que se deberán implementar para dicha protección, por lo que se buscará de igual modo implementarlo y mantenerlo actualizado.

5) Acciones preventivas en materia de protección de datos personales.

Posiblemente al ser un tema amplio, importante y que hasta el día de hoy es novedoso debemos poner en marcha las acciones y estrategias para poder así cumplir con lo establecido por la Ley General de Protección de Datos Personales; en razón de ello y en términos de lo dispuesto por dicho ordenamiento, la Unidad de Transparencia, como encargada de vigilar y coordinar que las disposiciones previstas por la Ley General de Transparencia y Acceso a la Información Pública y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados se atiendan en los términos y plazos establecidos; deberá establecer como actividad interrelacionada, el monitoreo y la revisión anualmente de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales tratados dentro de la SEDATU; del mismo modo, deberá implementar las acciones

Av. Heroica Escuela Naval Militar Número 701, Colonia Presidentes Ejidales Segunda Sección, Coyoacán, C.P. 04470 Tel: 55 68209700
www.gob.mx/sedatu





preventivas y necesarias que garanticen la protección de los datos personales en posesión de la Secretaría, tendientes a minimizar los riesgos inherentes a su tratamiento.

Líneas estratégicas:

1) Sensibilización y capacitación sobre la protección de los datos personales.

Les corresponde a todas las personas servidoras públicas y/o personal de la Administración Pública y en particular de la Secretaría de Desarrollo Agrario, Territorial y Urbano, que recaban datos personales, protegerlos para que los titulares de los mismos eviten estar en situación de vulnerabilidad o riesgo por el mal uso, acceso, trato y/o almacenamiento de los mismos.

Para lograrlo, el presente programa pretende sensibilizar y capacitar a todo el personal y/o personas servidoras públicas de la SEDATU, respecto de todos los aspectos relativos a la protección de datos personales, sin importar si son sujetos que traten o no datos personales.

Por ello, esta primera estrategia ataca la problemática de la existencia del desconocimiento del tema de la protección de los datos personales, así como del temor de la población de que usen sus datos de manera indebida, en relación con el ejercicio de los derechos ARCO.

Nº	LÍNEAS DE ACCIÓN	RESPONSABLE	META	FECHA TENTATIVA	EVIDENCIA
1.-	Campaña de sensibilización y conocimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y normatividad aplicable.	Dirección de la Unidad de Enlace con el INAI	Envío de 30 infografías a través del correo de la Unidad de Transparencia a todas las personas servidoras públicas.	Enero-diciembre de cada año.	Impresión de comunicados
2.-	Capacitación en materia de protección de datos personales.	Dirección de la Unidad de Enlace con el INAI Todos las personas servidoras públicas de la SEDATU	Personal 100% capacitado en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.	Enero-diciembre de cada año.	Constancias





2) Fortalecimiento Institucional

Al ser la SEDATU un sujeto obligado, tiene el deber y la obligación de cumplir con toda la normatividad aplicable en materia de protección de datos personales; lo cual implica un trabajo constante y en equipo el que se debe implementar para cumplir con las obligaciones que tiene la SEDATU.

Nº	LÍNEAS DE ACCIÓN	RESPONSABLE	META	FECHA TENTATIVA	EVIDENCIA
1.-	Nombramiento de un enlace de datos personales por cada unidad responsable.	Dirección de la Unidad de Enlace con el INAI Unidades responsables de la Secretaría	100 % de enlaces designados.	Enero-marzo de cada año.	Oficio de designación
2.-	Aperturar una bitácora con la finalidad de llevar un registro de las vulneraciones que existan, atendiendo lo dispuesto por el diverso 39 de la multicitada Ley General	Dirección de la Unidad de Enlace con el INAI	Bitácora aperturada	Julio de 2021.	Bitácora aperturada
3.-	Solicitar a las unidades responsables notifiquen en su caso, alguna vulneración de datos personales.	Dirección de la Unidad de Enlace con el INAI Unidades responsables de la Secretaría	Oficio enviado a las Unidades Responsables Notificación vía oficio en caso de vulneración	Septiembre de 2021 Cada que ocurra una vulneración	Oficio Oficio
4.-	Notificar a la Dirección de la Unidad de Enlace con el INAI los nuevos inventarios de datos personales.	Dirección de la Unidad de Enlace con el INAI Unidades responsables de la Secretaría	Inventario actualizado	Actividad permanente	Oficio Inventario actualizado

Es importante indicar que se considerarán como **vulneraciones de seguridad**, en cualquier fase del tratamiento de datos, las siguientes:

- La pérdida o destrucción no autorizada;





- El robo, extravío o copia no autorizada;
- El uso, acceso o tratamiento no autorizado, o
- El daño, la alteración o modificación no autorizada

Por lo que, será importante considerar que las personas responsables de los sistemas de tratamiento de los datos personales que poseen, deberán de notificar inmediatamente a sus respectivos enlaces de protección de datos personales, cuando se actualice alguno de los puntos considerados anteriormente, debiendo contener lo siguiente:

- La naturaleza del incidente o vulneración ocurrida;
- Los datos personales comprometidos;
- Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
- Las acciones correctivas realizadas de forma inmediata;
- La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente, y
- Cualquier otra información que considere conveniente para apoyar a los titulares.

Después, el enlace de protección de datos personales, deberá de notificarlo a la Dirección de Enlace con el INAI, para que este lo informe al personal encargado de monitorear y revisar la eficacia y eficiencia del Programa de Protección de Datos Personales.

3) Implementación, revisión y mejora de las acciones diseñadas para el tratamiento y seguridad de los Datos Personales.

La SEDATU, a través de la Unidad de Transparencia ha integrado diversos documentos para el tratamiento y seguridad de los datos personales, los cuales deben ser implementados, revisados y mejorados de forma periódica.

1.- La SEDATU al ser un sujeto obligado, tiene el deber de crear **políticas internas para la gestión y tratamiento de los datos personales**, por lo cual las mismas fueron aprobadas por el Comité de Transparencia en la 8ª Sesión Extraordinaria, celebrada el 04 de mayo del 2021. De igual forma cuenta con las Políticas de SEDATU para facilitar la obtención de información y el ejercicio del derecho de acceso a la información, aprobadas por el Comité de Transparencia el 11 de marzo de 2021, en la 3ª Sesión Ordinaria del Comité de Transparencia.

2.- Todas y cada una de las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un **Sistema de Gestión**, entendiéndolo como el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en LGPDPPSO y las demás disposiciones que le resulten aplicables en la materia.

Al respecto, ese Sistema de Gestión, deberá ser aprobado por el Comité de Transparencia de la SEDATU para que sea de aplicación inmediata y cumpla también con el objetivo de identificar y gestionar la seguridad de los datos personales a efecto implementar las acciones que garanticen la protección de los datos personales en posesión de la Secretaría, tendientes a minimizar los riesgos inherentes a su tratamiento, buscando la mejora continua.





3.- Respecto al deber de elaborar un **Documento de Seguridad**, el cual será el instrumento que describa 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; es menester repetir que dicho documento fue elaborado por la Dirección de Enlace con el INAI y fue aprobado por el mencionado Comité de Transparencia, en la 5ª Sesión Ordinaria, llevada a cabo el 12 de mayo de 2021; y el mismo contiene:

- a) Los inventarios de datos personales y de los sistemas de tratamiento
- b) Las funciones y obligaciones de las personas que traten datos personales;
- c) El análisis de riesgos;
- d) El análisis de brecha;
- e) El plan de trabajo;
- f) Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
- g) El programa general de capacitación.

Asimismo, y de conformidad con la LGPDPSO dicho documento podrá sufrir actualizaciones considerando los siguientes eventos:

- I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
- II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
- III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
- IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Mejora del Programa de Protección de Datos Personales:

Con la finalidad de comprobar el cumplimiento del programa, la Dirección de Enlace con el INAI realizará las siguientes acciones:

1. Realizará al cierre de cada ejercicio un informe de los resultados del programa.
 2. El Comité de Transparencia con base en los resultados podrá modificar el programa.
 3. La Dirección de Enlace con el INAI realizará las recomendaciones que estime conveniente en materia de protección de datos personales, teniendo como finalidad fundamental que las unidades administrativas adopten acciones preventivas y correctivas.
- ✓ Acciones preventivas (deberán documentarse): Las **encaminadas a evitar** cualquier incumplimiento a lo establecido en el presente Programa, por lo que se podrán llevar las siguientes actividades:

- a) Analizar y revisar las posibles causas de incumplimiento;





- b) Determinar qué otras causas de incumplimiento podría desencadenarse a partir de ciertas situaciones de riesgo para el tratamiento de datos personales;
 - c) Evaluar las acciones necesarias para evitar que el incumplimiento ocurra;
 - d) Determinar e implementar estas acciones;
 - e) Documentar los resultados de las acciones tomadas , y
 - f) Revisar la eficacia de las acciones preventivas tomadas.
- ✓ Acciones correctivas (deberán documentarse): Las **encaminadas a eliminar las causas** de incumplimiento con relación a lo previsto en este documento o reducir su grado de prevalencia; se podrán llevar a la siguientes actividades:
- a) Analizar y revisar el incumplimiento;
 - b) Determinar las causas que dieron origen al incumplimiento;
 - c) Evaluar las acciones necesarias para evitar que el incumplimiento vuelva a ocurrir;
 - d) Proponer acciones y establecer un plazo para su cumplimiento;
 - e) Documentar resultados de las acciones tomadas , y
 - f) Revisar la eficacia de las acciones correctivas tomadas.

DIRECTORIO

Miguel Ángel Cancino Aguilar

Titular de la Unidad de Asuntos Jurídicos de la SEDATU
y Presidente del Comité de Transparencia.

Jesús María de la Torre Rodríguez

Titular del Órgano Interno de Control en la SEDATU
y miembro integrante del Comité de Transparencia.

Luis Humberto Ramírez Valenzuela

Director General de Recursos Materiales y Servicios Generales
y Coordinador de Archivos , así como miembro integrante del Comité de Transparencia.

Francisco Javier Dorantes Díaz

Director General de Legislación, Consulta y Pago de Predios
y suplente del Presidente del Comité de Transparencia.

Miguel Ángel Serrano Sánchez

Titular del Área de Responsabilidades en la SEDATU
y suplente del Titular del Órgano Interno de Control

René Conde Ayala

Titular de la Dirección de Servicios
y suplente del Director General de Recursos Materiales y Servicios Generales

Oralia Reséndiz Márquez

Directora de la Unidad de Enlace con el INAI y Secretaría del Comité de Transparencia





En cumplimiento a lo dispuesto en el artículo 30 fracción II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y para su debido cumplimiento por parte del personal de la Secretaría de Desarrollo Agrario, Territorial y Urbano, se autoriza el presente Programa de Protección de Datos Personales con fecha 30 de junio de dos mil veintiuno por el Comité de Transparencia.

DR. FRANCISCO JAVIER DORANTES DÍAZ
DIRECTOR GENERAL DE LEGISLACIÓN,
CONSULTA Y PAGO DE PREDIOS, DE LA
UNIDAD DE ASUNTOS JURÍDICOS, EN SU
CARÁCTER DE SUPLENTE DEL PRESIDENTE
DEL COMITÉ DE TRANSPARENCIA

LIC. MIGUEL ÁNGEL SERRANO SÁNCHEZ
TITULAR DEL ÁREA DE
RESPONSABILIDADES EN SU CARÁCTER
DE SUPLENTE DEL TITULAR DEL ÓRGANO
INTERNO DE CONTROL EN LA
SECRETARÍA DE DESARROLLO AGRARIO,
TERRITORIAL Y URBANO, EN SU
CARÁCTER DE INTEGRANTE DEL COMITÉ
DE TRANSPARENCIA.

LIC. RENÉ CONDE AYALA
TITULAR DE LA DIRECCIÓN DE SERVICIOS,
EN SU CARÁCTER DE SUPLENTE DEL
TITULAR DE LA DIRECCIÓN GENERAL DE
RECURSOS MATERIALES Y SERVICIOS
GENERALES Y COORDINADOR DE
ARCHIVOS, INTEGRANTE DEL COMITÉ DE
TRANSPARENCIA.

LIC. ORALIA RESÉNDIZ MARQUEZ
DIRECTORA DE LA UNIDAD DE ENLACE CON EL INAI,
SECRETARIA TÉCNICA DEL COMITÉ DE TRANSPARENCIA

