



GOBIERNO DE
MÉXICO

AGRICULTURA



SENASICA

PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES

SERVICIO NACIONAL DE SANIDAD,
INOCUIDAD Y CALIDAD
AGROALIMENTARIA

**ÍNDICE**

	Página
PRESENTACIÓN	3
I. MARCO NORMATIVO	3
II. ALCANCE	4
III. OBJETIVOS	4
IV. LÍNEAS ESTRATÉGICAS	4
1. Sensibilización	4
2. Desarrollo de competencias	5
3. Implementación, operación, revisión, supervisión y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales	5
V. DESARROLLO DE LÍNEAS ESTRATÉGICAS	5
1. Sensibilización	5
2. Desarrollo de competencias	6
a) Principios: Licitud, Lealtad, Consentimiento, Información, Proporcionalidad, Finalidad, Calidad y Responsabilidad	7
b) Deberes: Confidencialidad y Seguridad	11
c) Inventario de datos personales y sistemas de tratamiento	13
d) Aviso de Privacidad	13
e) Derechos ARCO	16
f) Transferencias	17
g) Documento de Seguridad	18
h) Vulneraciones	18
3. Implementación, operación, revisión, supervisión y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales.	19
VI. GLOSARIO DE TÉRMINOS	19



PRESENTACIÓN

Con la reforma del artículo 6o Constitucional en 2014 se fijan las bases para la emisión de una Ley General respecto de la información en posesión de entes públicos.

El 26 de enero de 2017 se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPO), 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 en posesión de los organismos de los poderes Ejecutivo, Legislativo y Judicial en los tres niveles de gobierno.

Asimismo, el 26 de enero de 2018, se publicaron los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en los que se enuncian las obligaciones exigibles de tratamiento de datos personales y el ejercicio de los derechos (ARCO), a partir de ambas publicaciones el sujeto obligado obtiene la figura jurídica del "Responsable" que debe actuar de conformidad con los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, además de adoptar medidas de seguridad (administrativas, físicas y técnicas) en el tratamiento de datos personales.

El 28 de septiembre de 2018, se publicó en el Diario Oficial de la Federación el Decreto por el que se promulgan el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal ("Convenio 108") y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos. Dicho decreto entró en vigor el día primero de octubre de ese año, con lo cual el Convenio 108 y su Protocolo son vinculantes para México a partir de esa fecha. Asimismo, México ha suscrito diversas convenciones, tratados y acuerdos en la materia, y participa en diversas iniciativas, destacando la Red Iberoamericana de Protección de Datos (RIPD).

Bajo ese contexto, el Servicio Nacional de Sanidad, Inocuidad y Calidad Agroalimentaria (SENASICA), órgano desconcentrado de la Secretaría de Agricultura y Desarrollo Rural (SADER) es un sujeto obligado reconocido por la LGPDPPO y tiene la obligación de cumplir con lo dispuesto en el marco normativo aplicable.

I. MARCO NORMATIVO

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

- Constitución Política de los Estados Unidos Mexicanos.
- Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108) y su Protocolo adicional.
- Ley General de Transparencia y Acceso a la Información
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley General de Responsabilidades Administrativas de los Servidores Públicos
- Ley Orgánica de la Administración Pública Federal.
- Ley General del Sistema Nacional de Seguridad Pública.



- Ley General de Archivos.
- Reglamento Interior de la SADER.
- Reglamento Interior del SENASICA.
- Lineamientos Generales de Protección de Datos Personales en Sector Público

El Programa de Protección de datos Personales, es una herramienta de las acciones mínimas que deberá considerarse para la eficaz protección de datos personales recabados en la atención de las atribuciones de cada unidad administrativa del SENASICA. Este conjunto de esfuerzos y acciones se ajustan a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y al marco normativo aplicable.

II. ALCANCE

El presente Programa de Protección de Datos Personales, es de observancia obligatoria para todas las unidades administrativas del SENASICA, que en el cumplimiento de sus atribuciones recaban y tratan datos personales.

También aplicará a todos los servidores públicos que en el desarrollo de sus funciones realicen algún tipo de tratamiento de datos personales. En este caso, están obligados a conocer y aplicar las medidas de seguridad mínimas establecidas en la LGPDPPSO y sus Lineamientos Generales.

Se destaca que la responsabilidad de la tarea, implica no sólo tratar los datos personales con responsabilidad, sino también, guardar la debida confidencialidad y garantizar seguridad sobre la información a la que tengan acceso.

III. OBJETIVOS

El programa tiene como objetivos:

Cumplir con las obligaciones que establecen la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales, así como la normatividad que derive de los mismos.

Establecer las directrices y herramientas necesarias, para garantizar la protección de los datos personales en posesión de las unidades administrativas, por medio de la sensibilización, capacitación, implementación, operación, revisión, vigilancia y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales.

IV. LÍNEAS ESTRATÉGICAS

Lo anterior, se logrará mediante la ejecución de las líneas estratégicas que a continuación se señalan:

1. Sensibilización

Para aumentar el nivel de conocimiento de los servidores públicos del SENASICA, la Unidad de Transparencia difundirá a través del correo electrónico institucional infografías relativas a la protección de datos personales abordando temas de confidencialidad, seguridad, avisos de privacidad, entre otros.

El incremento constante del conocimiento en la materia tiene como finalidad colocar en el dominio de las personas servidoras públicas, los temas más básicos sobre la protección de los datos personales.



2. Desarrollo de Competencias

Para lograr la ejecución de esta línea estratégica la Unidad de Transparencia, realizará de manera constante al interior del SENASICA, campañas de promoción y difusión de diversos materiales sobre la protección de datos personales a través del correo electrónico institucional.

La Unidad de Transparencia, tomará en cuenta la oferta que brinda el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), para difundir a los servidores públicos la calendarización sobre los diversos temas de capacitación en materia de protección de datos personales, con la finalidad de que los servidores públicos estén debidamente capacitados en la normatividad de referencia.

Bajo ese contexto, los servidores públicos que participen y se involucren en los temas de capacitación que engloba la LGPDPPSO, podrán contar con información certera sobre el cumplimiento y atención de sus obligaciones en materia de protección de datos personales, dando cumplimiento a los deberes y principios previstos en la normatividad, dado que el tema de protección de datos personales es competencia de todos los servidores públicos que participen y se involucren en la protección de la información confidencial que obre en los archivos, sistemas y bases de datos de la institución.

3. Implementación, operación, revisión, supervisión y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales.

Es fundamental que las personas servidoras públicas tengan pleno dominio de las obligaciones, en cuanto a la elaboración de los inventarios de tratamiento, de avisos de privacidad y del Documento de Seguridad, así como realizar acciones de revisión, supervisión y de mejora continua del Programa con base en los resultados de las verificaciones que realice la Unidad de Transparencia y el INAI.

El documento de seguridad, deberá ser desarrollado por la Dirección de Tecnologías de la Información, con apoyo de cada unidad administrativa, entendiéndolo como el documento que da cuenta de las medidas técnicas, físicas y administrativas, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales en poder de la Institución.

V. DESARROLLO DE LÍNEAS ESTRATÉGICAS

1. Sensibilización

El Diccionario de la Lengua Española, define el concepto sensibilizar, como "hacer sensible a alguien" y efectivamente, el presente Programa, aspira lograr sensibilizar a las y los servidores públicos del SENASICA; es decir, contar con el conocimiento y compromiso de la profunda relevancia que tienen los datos personales.

Lo anterior, muestra que corresponde a todas las personas servidoras públicas de la Administración Pública Federal, y en particular del SENASICA, asumir el compromiso de velar en todo momento por el adecuado tratamiento de los datos personales recabados.



Para lograrlo, en el presente Programa se encuentra el conjunto de actividades necesarias para concientizar a las personas servidoras públicas, respecto de los diferentes aspectos relativos a la protección de datos personales, vistos desde la trascendencia del respeto a los derechos fundamentales.

El derecho a la autodeterminación informativa es un elemento que le permite al titular de los datos, decidir conscientemente con quién o qué organización desea compartir su información, así como tener la garantía que estarán adecuadamente protegidos. Desde luego que también se debe atender a las excepciones determinadas por el marco normativo.

Es importante tener presente que en la conmemoración del Día Internacional de la Protección de Datos Personales (28 de enero) se tiene como objetivo crear conciencia en autoridades de protección de datos, sujetos obligados y, primordialmente, entre los adultos, jóvenes y niños, acerca de la importancia de proteger, promover y difundir su derecho a la privacidad, así como destacar la importancia que tiene la protección de datos personales como un derecho humano consagrado en la legislación mexicana y en diversos instrumentos internacionales.

La campaña de sensibilización, ofrece información específica que ayudará a servidoras y servidores públicos de las unidades administrativas del SENASICA, a delinear acciones particulares para el diseño de procesos orientados a la protección de datos personales.

Con esta campaña, (las fechas se irán ajustando de acuerdo a las necesidades institucionales) se busca eliminar aquellos obstáculos que impiden el conocimiento de los principales componentes del marco normativo, reforzando la referencia implícita o explícita de que resulta fundamental entender el compromiso que tenemos como ciudadanos y ciudadanas, y como servidoras y servidores públicos, en una institución dedicada a la sanidad animal, vegetal, acuícola y pesquera. De suyo, la campaña de sensibilización también atiende a todos los elementos gráficos institucionales que, seguramente, podrán reforzar el sentimiento de pertenencia, identidad y comunidad con el movimiento nacional y global de marcos regulatorios, cada vez más exigentes en la protección de datos personales.

2. Desarrollo de competencias

El SENASICA, ha cumplido con toda la normatividad aplicable, en la materia de protección de datos personales. En tal sentido, la Unidad de Transparencia se ha ocupado de sensibilizar y de asesorar al personal de las unidades administrativas sobre la importancia de elaborar versiones públicas de documentos que contienen datos personales, elaborar avisos de privacidad y atender solicitudes de acceso a la información y de ejercicio de derechos ARCO.

Asimismo, las unidades administrativas están en conocimiento de que cuentan con las asesorías necesarias en dicha materia con el apoyo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y de la Unidad de Transparencia, para fortalecer y consolidar la asistencia a través del presente Programa, a efecto de que dichas unidades reciban la capacitación integral que les permita no sólo actualizar conocimientos en las tareas más relevantes de la protección de los datos personales, sino también identificar las buenas prácticas sobre la materia.

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, generando una conciencia institucional sobre la trascendencia del tratamiento y la protección de los datos personales que obran en las bases de datos o documentos institucionales.

Lo anterior, coadyuva a establecer procesos operativos internos (físicos o automatizados) aplicados a los datos personales relacionados, de manera enunciativa más no limitativa, con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, transferencia y en general cualquier uso o disposición de datos personales. En este sentido, el presente Programa ha sido aprobado por el Comité de Transparencia del SENASICA.

Las personas servidoras públicas responsables de los sistemas de tratamiento de datos personales que poseen, deberán de adoptar las medidas necesarias para evitar que se vulneren los mismos, respetando los principios de la protección de datos que constituyen el pilar mediante el cual se articula este derecho y son de observancia obligatoria para todo aquél que interviene en el tratamiento de datos personales desde el momento de la obtención hasta la destrucción de los mismos. A la luz de lo anterior, se describen los siguientes principios y deberes:

a) Principios

a.1) Principio de licitud

El principio de licitud significa que las personas servidoras y servidores públicos 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 la normatividad aplicable les confiera.

a.2) Principio de lealtad

De acuerdo con el principio de lealtad, las personas servidoras públicas no podrán recabar datos personales 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 contra los titulares.
- No se vulnere la confianza del titular en relación con que sus datos personales serán tratados conforme a lo acordado; y
- Se informen todas las finalidades del tratamiento en el aviso de privacidad.

a.3) Principio del consentimiento

Como regla general, las personas servidoras y servidores públicos deberán contar con el consentimiento del titular para el tratamiento de los 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, además de que debe ser libre tal y como lo refiere la LGPDPPSO, en el sentido que no medie error, mala fe, violencia o dolo que afecten la voluntad del titular.

a.4) Principio de información

Por 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 el 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.

Es importante tomar en cuenta que con independencia de que se requiera o no el consentimiento del titular para el tratamiento de sus datos personales, el responsable está obligado a poner a su disposición el aviso de privacidad.

a.5) principio de proporcionalidad

El principio de proporcionalidad establece la obligación a las personas servidoras pública tratarán aquellos datos personales que resulten necesarios, adecuados y relevante de acuerdo a las finalidades para las cuales se obtuvieron. De acuerdo con lo antes expuesto, se realizarán las siguientes obligaciones en torno al principio de proporcionalidad:

Tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron;

- Limitar al mínimo posible el periodo de tratamiento de datos personales sensibles; y
- Crear bases de datos con datos personales sensibles sólo cuando se cuente con el consentimiento expreso de su titular o,
- en su defecto, se trate de los casos establecidos en el artículo 22 de la Ley General en la materia.

Atendiendo a lo anterior las personas servidoras públicas deberán de realizar el esfuerzo para que los datos personales tratados sean los mínimos necesarios para lograr la o las finalidades para las cuales se obtuvieron, mismas que deben ser acordes con las atribuciones conferidas al responsable y señaladas en el aviso de privacidad.

a.6) Principio de finalidad

Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales, y solo pueden ser tratados para cumplir con la finalidad 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, explícitas, lícitas y legítimas, siendo importante que las personas servidoras públicas consideren lo siguiente:



- **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:** Tienen lugar 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 mexicana y el derecho internacional que le resulte aplicable.
- **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.

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.

a.7) Principio de calidad

El 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.

Las personas servidoras públicas están obligadas 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;
- Bloquear 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;
- 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.

A efecto de cumplir con el principio de calidad, es necesario tomar en consideración los siguientes aspectos:

- 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;
- Las disposiciones aplicables en la materia de que se trate;
- Los aspectos administrativos, contables, fiscales, jurídicos información, y
- El periodo de bloqueo.

Es importante señalar que, en particular, el artículo 24 de la Ley General de Archivos, establece que se deben documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales respecto de cada tratamiento que se efectúe por las unidades administrativas.

- Conclusión del plazo de conservación

Una vez concluido el plazo de conservación, y siempre que no exista disposición legal o reglamentaria que establezca lo contrario, las unidades administrativas deben proceder a la supresión de los datos personales. En este caso, deberán de informarlo a la Unidad de Transparencia, quien lo hará del conocimiento del Comité de Transparencia, a efecto de que determine lo conducente. Es importante recordar que el plazo de conservación debe incluir un periodo de bloqueo, ya que los datos personales deben ser bloqueados antes de que sean eliminados o suprimidos.

Además, en cuanto a los datos personales sensibles, el responsable debe realizar esfuerzos razonables para limitar el periodo de tratamiento al mínimo indispensable.

- Bloqueo de los datos personales

El bloqueo 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. Las personas servidoras públicas están obligadas a:

- Bloquear 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.

a.8) Principio de responsabilidad

El principio de responsabilidad cierra el círculo en relación con los principios, deberes y obligaciones, así mismo establece la obligación de las unidades administrativas a cumplir el resto de los principios, adoptar las medidas necesarias para su aplicación y demostrar ante titulares y el INAI, que cumple con sus obligaciones en materia de protección de los datos personales. Bajo este principio, las personas servidoras públicas responsables del tratamiento están obligados a velar por la protección de los datos personales aún y cuando los datos estén siendo tratados por encargados.

Asimismo, este principio supone que se tomen las medidas suficientes para que los términos establecidos en el aviso de privacidad y sean respetados por aquéllos con los que mantenga una relación jurídica, así como al momento de realizar transferencias nacionales o internacionales de datos personales. Finalmente,



han quedado expuestos los principios que deberán de considerar, las unidades administrativas para dar cumplimiento al marco normativo.

b) Deberes

La protección de los datos personales además de principios y obligaciones encuentra base en dos deberes:

b.1) Deber de confidencialidad

Por confidencialidad, se entiende que se deben de establecer controles o mecanismos que tengan por objeto que todas aquellas personas servidoras públicas 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.

Las personas servidoras públicas 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 ésta.

b.2) 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 tomando en consideración los estándares nacionales e internacionales, en materia de protección de datos personales y seguridad.

En este sentido, las personas servidoras públicas con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, deberán establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la promoción de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, seguridad y disponibilidad de los datos de carácter personal que conozca y a los que tenga acceso con motivo de la relación laboral que mantenga con la Institución debiendo subsistir esta obligación sus relaciones con ésta.

Es importante recordar que un dato personal es cualquier información correspondiente a una persona física identificada o cuya identidad se pueda conocer a través de esa información, por ejemplo, nombre, apellidos, CURP, número de pasaporte, número de teléfono, dirección de correo electrónico, número de tarjeta de crédito, datos profesionales, laborales o académicos, salario, entre otros

A continuación, se describen las siguientes categorías de datos personales y sus niveles:

- Datos identificativos: Nombre, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Clave de elector, Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía y demás análogos. Nivel: (básico)



- Datos electrónicos: Las direcciones electrónicas, tales como, el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre de usuario, contraseñas, firma electrónica; o cualquier otra información empleada por la persona, para su identificación en Internet, acceso a sistemas de información u otra red de comunicaciones electrónicas; Nivel: (básico)
- Datos laborales: Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio y demás análogos. Nivel: (básico)
- Datos académicos: Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos y demás análogos. Nivel: (básico)
- Datos de salud: El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona. Nivel: (alto)
- Datos patrimoniales: Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, flanzas, servicios contratados, referencias personales y demás análogos. Nivel: (medio)
- Datos sobre procedimiento administrativos: La información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del derecho. Nivel: (medio)
- Datos de tránsito y movimientos migratorios: Información relativa al tránsito de personas dentro y fuera del país, así como información migratoria. Nivel: (básico)
- Datos biométricos: huellas dactilares, ADN, geometría de la mano, características de iris y retina y demás análogos. Nivel: (alto)
- Datos sensibles: origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas, la pertenencia a sindicatos, la salud y preferencia sexual. Nivel: (alto)
- Datos personales de naturaleza pública: aquellos que por mandato legal sean accesibles al público. Nivel: (básico)

Se deberán de considerar los siguientes atributos y el o los medios de almacenamiento, físicos y/o electrónicos en los que se encuentren datos personales:

- Irreversibilidad: que el proceso utilizado no permita recuperar los datos personales.
- Seguridad y confidencialidad: que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la Ley General y los Lineamientos Generales.
- Favorable al medio ambiente: que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.



A mayor abundamiento, cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso.

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

c) Inventario de datos personales y sistemas de tratamiento.

Este último, deberá ser desarrollado por las unidades administrativas que traten datos personales con el apoyo de la Unidad de Transparencia en el documento de seguridad, entendiendo este último, como el documento que da cuenta de las medidas técnicas, físicas y administrativas, para garantizar la confidencialidad, integridad y disponibilidad de personales que obran en poder de las diversas unidades administrativas, asimismo de seguridad se contiene el inventario de datos personales.

d) Aviso de Privacidad

El aviso de privacidad es el documento que las unidades administrativas deberán poner a disposición del titular de forma física, electrónica o en cualquier formato, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

La puesta a disposición del aviso de privacidad implica que éste se publique en un lugar visible, accesible y gratuito, en el cual el titular, de manera informada, cuente con la posibilidad de conocer el tratamiento que se les dará a sus datos personales. En todo caso, el aviso de privacidad deberá estar ubicado en un lugar visible y que facilite su consulta, los que se encuentran disponibles en la página web institucional.

Lo anterior, con el propósito de que las personas servidoras públicas, tengan conocimiento sobre el tratamiento de datos personales que serán transferidos con motivo de algún curso, taller, capacitación que realicen las unidades administrativas atendiendo a las atribuciones señaladas en el Reglamento Interior.

Finalmente, las personas servidoras públicas con apoyo de los enlaces designados en la materia, deberán considerar que los avisos de privacidad, se harán del conocimiento al Comité de Transparencia de conformidad con lo establecido en el artículo 84 de LGPDPPSO, por ser la máxima autoridad en la materia de protección de datos personales.

d.1 Modalidades del Aviso de Privacidad

Existen dos modalidades del aviso de privacidad: simplificado e integral. El simplificado debe contener lo siguiente:

- La denominación del responsable;
- Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular;



- Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:

a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y

b) Las finalidades de estas transferencias;

- Los mecanismos y medios disponibles para que el titular, en su caso pueda manifestar su negativa para el tratamiento de sus datos en aquellas finalidades y transferencias que requieren el consentimiento del titular, y
- El sitio donde se podrá consultar el aviso de privacidad integral

Por otra parte, el aviso de privacidad integral deberá contener, además de lo citado con anterioridad, al menos, la información siguiente:

- El domicilio del responsable;
- Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;
- El fundamento legal que faculta al responsable para llevar a cabo el tratamiento; Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular;
- Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;
- El domicilio de la Unidad de Transparencia, y
- Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

Finalmente, para conocer los formatos de aviso de privacidad que deberán utilizar las unidades administrativas, se agregan al presente Programa las plantillas de los avisos de privacidad simplificado e integral.

d. 2 Medidas Compensatorias

Las medidas compensatorias son los mecanismos alternos para dar a conocer a los titulares el aviso de privacidad simplificado, a través de su difusión por medios masivos de comunicación u otros mecanismos de amplio alcance.

Para dar a conocer a los titulares el aviso de privacidad simplificado, a través de su difusión por medios masivos de comunicación u otros mecanismos de amplio alcance, como los siguientes:

- Diario Oficial de la Federación o diarios de circulación nacional;
- Página de Internet o cualquier otra plataforma o tecnología oficial del responsable;
- Carteles informativos;
- Cápsulas informativas radiofónicas, o
- Cualquier otro medio alternativo de comunicación masivo.



Ahora bien, de conformidad con el artículo 2 de los Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal, se entiende por imposibilidad, esfuerzos desproporcionados y obtención directa, lo siguiente:

- **Imposibilidad de dar a conocer al titular el aviso de privacidad de forma directa:** se presenta cuando el responsable no cuenta con los datos personales necesarios que le permitan tener un contacto directo con el titular, ya sea en sus archivos, registros, expedientes, bases o sistemas de datos o bien, porque los mismos se encuentran desactualizados, incorrectos o inexactos.
- **Esfuerzos desproporcionados para dar a conocer al titular el aviso de privacidad en forma directa:** cuando el número de titulares sea tal, que el hecho de poner a disposición de cada uno de éstos el aviso de privacidad, de manera directa, le implique al responsable un costo excesivo atendiendo a su suficiencia presupuestaria, o comprometa la viabilidad de su presupuesto programado o la realización de sus funciones o atribuciones que la normatividad aplicable le confiera; o altere de manera significativa aquellas actividades que lleva a cabo cotidianamente en el ejercicio de sus funciones o atribuciones.
- **Obtención directa de los datos personales:** cuando el titular proporciona personalmente los datos personales a quien representa al responsable o a través de algún medio que permita la entrega directa como, sistemas o medios electrónicos, ópticos, sonoros, visuales, vía telefónica, internet o cualquier otra tecnología o medio físico.

Los avisos de privacidad serán actualizados o, en su caso, elaborados por cada unidad administrativa que trate datos personales, según sus atribuciones.

d.3 Consentimiento

Las personas servidoras públicas deberán de contar con el consentimiento del titular de los datos personales, salvo que se actualice alguna de las excepciones de los artículos 22, 66 y 70 de la LGPDPPSO. Antes de poner a disposición del titular el aviso de privacidad, la unidad administrativa deberá observar lo siguiente:

- Elaborar su respectivo aviso de privacidad, revisando la necesidad y legalidad de su tratamiento para cumplir con la finalidad de que se trate, a fin de que quede debidamente justificada la obtención y uso de los datos personales.
- Identificar las finalidades para las cuales se requiere el consentimiento de los titulares.
- En caso de que las finalidades o tratamiento establecidos en el aviso de privacidad, encuadre en las hipótesis de los artículos 22, 66 y 70 de la LGPDPPSO, la unidad administrativa estará exenta de solicitar al usuario su consentimiento.
- Una vez que se ponga a disposición del titular el aviso de privacidad, las unidades administrativas deberán observar los casos en que se requiera consentimiento tácito o expreso, dependiendo el tipo de datos personales.



e) Derechos ARCO

El acrónimo ARCO está conformado por las iniciales de los derechos de Acceso, Rectificación, Cancelación y Oposición de los datos personales, derechos reconocidos por la legislación mexicana y que los titulares pueden ejercer, consisten en:

- **Derecho de Acceso:** Es el derecho que tiene el titular de solicitar el acceso a sus datos personales que se encuentran en las bases de datos, registros o expedientes del responsable que los posee resguardados, así mismo de conocer el tratamiento que se da a su información personal.
- **Derecho de Rectificación:** Es el 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. En otras palabras, puede solicitar a quien posea o utilice sus datos personales que los corrija cuando los mismos sean incorrectos, desactualizados o inexactos.
- **Derecho de Cancelación:** Es el 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 hay que tomar en cuenta que no en todos los casos se podrán eliminar los datos personales, principalmente cuando sean necesarios por alguna cuestión legal o para el cumplimiento de obligaciones.
- **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 éstas. También en este caso, como en el anterior, no siempre se podrá impedir el uso de los datos, cuando éstos sean necesarios por motivos legales o para el cumplimiento de obligaciones.

Las personas servidoras públicas, 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 o su ejercicio se verá limitado por cuestiones de seguridad nacional: orden, seguridad y salud públicos, así como por derechos de terceros.

Las causas por las que el responsable puede negar el ejercicio de los derechos ARCO son:

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

Cabe resaltar, aunque no proceda el ejercicio de derechos ARCO, las unidades administrativas están obligadas a responder la solicitud e informar las causas de improcedencia.



Luego entonces, 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, por lo que es indispensable acreditar la identidad.

f) Transferencias

Las personas servidoras públicas responsables del tratamiento de los datos personales deberán comprender que la transferencia es toda comunicación de datos personales, dentro o fuera del territorio nacional, a persona distinta del titular, del responsable o del encargado.

Es decir, la comunicación de datos entre el responsable y el encargado, NO se considera transferencia. A ese tipo de comunicaciones se les llama remisiones. Es importante señalar que los responsables no están obligados a solicitar el consentimiento de los titulares para la realización de remisiones, ni de informarlas en el aviso de privacidad, contrario a lo que ocurre con las transferencias, como se verá más adelante.

Para que las unidades administrativas transfieran los datos personales dentro o fuera de México, es necesario que se ajusten a lo siguiente:

- Se informe al titular en el aviso de privacidad el destinatario de las transferencias ya sea en el ámbito público o privado, además deberá señalar las finalidades de estas transferencias. En caso de ser una transferencia que requiera consentimiento, deberá habilitar los mecanismos correspondientes.
- El titular haya otorgado su consentimiento para que la transferencia se realice, salvo los casos de excepción previstos en los artículos 22, 66 y 70 de la Ley General (este tipo de transferencias es opcional incluirlas en el aviso de privacidad integral).

No se requerirá el consentimiento de los titulares para realizar transferencias, en los siguientes supuestos:

- Cuando una ley así lo disponga;
- Cuando las transferencias que se realicen entre responsables, sean para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento;
- Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
- Para el reconocimiento o defensa de derechos del titular ante autoridad competente;
- Para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica;
- Cuando exista una situación de emergencia;
- Asistencia sanitaria;
- Los datos se encuentren en fuentes de acceso público;
- Los datos personales sean sometidos a un procedimiento previo de disociación, o
- El titular de los datos sea una persona reportada como desaparecida
- Transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal;
- Transferencia sea internacional, en cumplimiento en una ley o tratado internacional suscrito y ratificado por el estado mexicano;



- A petición de una autoridad u organismo extranjero, competente en su carácter de receptor, cuyas facultades sean homologas;
- Transferencia necesaria por un contrato celebrado o por celebrar en interés del titular;
- La transferencia sea necesaria por razones de seguridad.

g) Documento de Seguridad

El documento de seguridad es el 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.

Para su elaboración resulta indispensable la participación de las personas servidoras publicas responsables del tratamiento de los datos personales en las unidades administrativas, en el ámbito de su competencia quienes, para este fin, serán coordinadas por el personal de la Unidad de Transparencia, quien orientará y verificará la integración del documento, mismo que se conformará por lo siguiente:

- El inventario de datos personales;
- Las funciones de las personas que tratan datos;
- El análisis de riesgos;
- El análisis de brecha;
- El Plan de Trabajo;
- Los mecanismos de monitoreo y revisión;
- El Programa de Capacitación.

El documento de seguridad, podrá sufrir actualizaciones considerando los siguientes eventos:

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

h) Vulneraciones

La vulneración de datos personales además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, 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



Las personas servidoras públicas responsables de los sistemas de tratamiento de los datos personales que poseen, deberán notificar inmediatamente a sus respectivos enlaces de protección de datos personales, cuando se actualice alguno de los puntos considerados anteriormente, debiendo informar 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;
- Los medios donde puede obtener más información al respecto;
- 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 y documentación que considere conveniente para apoyar a los titulares.

3. Implementación, operación, revisión, supervisión y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales.

Con la finalidad de comprobar el cumplimiento del Programa, el Comité de Transparencia requerirá en sesión ordinaria a la Unidad de Transparencia lo siguiente:

- El informe de resultados de los programas de sensibilización y desarrollo de competencias diseñadas para el adecuado tratamiento y la seguridad de los datos personales, es decir, el número de difusiones realizadas por correo electrónico, así como los resultados de capacitación y actualización y difusión de los avisos de privacidad.
- El informe de resultados de las verificaciones del órgano garante y, en su caso, las acciones para atender las observaciones o áreas de oportunidad sugeridas por éste.
- Informe sobre las medidas de seguridad física, administrativa y técnica, establecidas en el "Documento de Seguridad".

El Comité de Transparencia, 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.

VI. GLOSARIO DE TERMINOS

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

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



Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabadas, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;

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

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

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

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

Derechos 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 medidas de seguridad técnicas, físicas y administrativas adoptadas por el garantizar la confidencialidad, integridad y disponibilidad de los datos personal

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

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

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

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;





- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
- d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

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. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir que el acceso a las bases de datos o a la información, designando a usuarios identificados y autorizados;
- b) Generar un esquema de privilegios para que el usuario lleve a cabo actividades que requiere con motivo de sus funciones;
- c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
- d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.
- e) Programa: Programa de Protección de Datos Personales.

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

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

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

Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;

SENASICA: Servicio Nacional de Sanidad, Inocuidad y Calidad Agroalimentaria.

Titular: Persona física a quien corresponden los datos personales.

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

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro,




organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Unidad Administrativa: Área a la que se le confiere atribuciones específicas en el reglamento interno, estatuto orgánico o instrumento normativo equivalente.


COMITÉ DE TRANSPARENCIA



**ING. EDGAR RAFAEL ALARCÓN GONZÁLEZ
TITULAR DE LA UNIDAD DE TRANSPARENCIA**



**MRTO. MARCO ANTONIO FLORES CAMACHO
SUPLENTE DEL TITULAR DEL ÓRGANO INTERNO DE CONTROL EN LA SADER**



**MTRO. OMAR A. DEL REAL RENTERÍA
SUPLENTE DEL COORDINADOR DE ARCHIVOS EN EL SENASICA**