GUÍA PARA LA

PROTECCIÓN DE DATOS PERSONALES DE PERSONAS MIGRANTES EN POSESIÓN

DE ALBERGUES

OIM
ONU MIGRACIÓN

Publicado por:

Organización Internacional para las Migraciones (OIM)
Francisco Sosa #267, Col. Barrio de Santa Catarina, Coyoacán
C.P. 04010
Ciudad de México
México
Tel.: +52 55 5536 3922
E-mail: iommexico@iom.int
Website: www.mexico.iom.int

ISBN 978-92-9068-896-9 (Impreso)
ISBN 978-92-9068-897-6 (PDF)

Citación: Guía para la protección de datos personales de personas migrantes en posesión de albergues. Editorial, Cd. Mex.

PUB2020/081/R

CRÉDITOS
Equipo de investigación: Yolice Quero y Brenda Andazola de la Unidad de Protección.
Editor gráfico: Vinyl Design

Guía para la protección de datos personales de personas migrantes en posesión de albergues

ÍNDICE

Antecedentes

Siglas y Acrónimos

ANTECEDENTES

A principios de diciembre de 2019, en el marco de fortalecimiento técnico de albergues para personas migrantes, la Organización Internacional para las Migraciones (OIM) impartió talleres en Ciudad Juárez y Tijuana sobre la gestión de alojamientos temporales, donde se incluyó una sesión acerca de la protección de datos personales. Esta sesión tuvo como finalidad:

- Generar consciencia sobre la importancia en el manejo correcto de datos personales.
- Identificar los riesgos de protección que enfrentan las personas migrantes cuando sus datos personales reciben un tratamiento indebido.
- Compartir nociones básicas del marco normativo mexicano que regula la materia.
- Realizar un inventario de datos personales recolectados por los albergues y mapear el tratamiento que se le dan a los mismos.

En seguimiento a los talleres, la OIM pone a disposición la presente guía con la finalidad de brindar una herramienta práctica que la oriente y permita a los albergues generar un protocolo de protección de datos personales en conformidad con las reglas y obligaciones mínimas en la materia, fomentando los derechos y la integridad de las personas migrantes.

SIGLAS Y ACRÓNIMOS

CPEUM	Constitución Política de los Estados Unidos Mexicanos
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
OIM	Organización Internacional para las Migraciones

Introducción

Cómo utilizar la Guía

INTRODUCCIÓN

En actividades cotidianas, los albergues obtienen y administran diferentes datos de las personas migrantes que hospedan y asesoran cada día, generándose una serie de obligaciones sobre la protección de los datos personales establecidas en el marco normativo mexicano.
La protección de datos personales es un derecho humano reconocido por la Constitución Política de los Estados Unidos Mexicanos (CPEUM), que establece que las personas son dueñas de sus datos personales y pueden disponer de la información sobre sí mismas, por lo que tienen el control y el poder de decidir sobre quién puede tratar sus datos y para qué fines (derecho de autodeterminación informativa), a la vez que tienen el derecho de acceder, rectificar, cancelar y oponerse sobre sus datos. En ese sentido, la protección de datos personales exige que quienes manejan este tipo de información cumplan con ciertas reglas mínimas para garantizar el derecho a la privacidad y que los datos sean tratados de manera lícita, leal y responsable.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y su reglamento establecen obligaciones a personas, ya sean físicas o morales[1], que manejan datos personales en sus actividades a fin de garantizar los derechos a la autodeterminación informativa, la privacidad y la seguridad de todas las personas. Entre las obligaciones legales puntualizamos:

- Informar a las personas sobre la información que se recaba de ellas y con qué fines, por medio de un aviso de privacidad.
- Contar con el consentimiento previo del titular sobre el tratamiento y/o transferencia de sus datos.
- Designar a una persona o departamento de datos personales.
- Guardar confidencialidad sobre los datos personales.
- Establecer y mantener medidas de seguridad administrativas, técnicas y físicas para proteger los datos personales[2].

A continuación, se presenta la guía para la protección de datos personales de personas migrantes en posesión de albergues, la cual se elaboró tomando como base el marco normativo mexicano, los lineamientos y recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y el Manual de Protección de Datos de OIM.

La presente guía sirve para la creación de mecanismos institucionales de protección de datos personales de personas migrantes.

[1] El artículo 2 de la LFPDPPP establece que son sujetos regulados por la ley "los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales", exceptuando a las sociedades de información crediticia y a las personas que recolecten o almacenen datos personales para uso exclusivamente personal y sin fines de divulgación o utilización comercial.
[2] El artículo 19 de la LFDPPP señala la protección contra el daño, la pérdida, la alteración, destrucción o el uso, acceso o tratamiento no autorizado.

CÓMO UTILIZAR LA GUÍA

La guía recoge normas, lineamientos y recomendaciones del INAI y de la OIM para que los albergues puedan gestionar e informar correctamente a las personas migrantes sobre la obtención, uso, almacenamiento, transferencia y eliminación de datos personales; brindando así herramientas para: a) elaborar el aviso de privacidad, b) obtener el consentimiento de los titulares, c) designar una persona o departamento de datos personales y d) desarrollar medidas de seguridad para la protección de datos personales.

En el cuerpo del documento, se insertan recuadros para advertir al lector de la existencia de recursos tales como guías, manuales o herramientas elaborados por el INAI o la OIM que pueden utilizarse para aplicar las recomendaciones que se presentan en el texto. Los recursos se identifican de la siguiente manera:

| Recursos

Esta guía cuenta con un glosario de conceptos básicos para consulta del lector tomados de la normatividad mexicana y los estándares de la OIM en la materia. Adicionalmente, destacamos algunos términos que consideramos claves, colocándolos en **negritas**, con la intención de que el lector realice una revisión de la definición legal en el glosario y obtenga una mejor comprensión del significado y alcance del término. Las palabras clave se identifican de la siguiente manera:

"Existen tres modalidades del **aviso de privacidad**: integral, simplificado y corto […]"

Marco Normativo

MARCO NORMATIVO

- Constitución Política de los Estados Unidos Mexicanos, Artículo 16.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.
- Lineamientos del Aviso de Privacidad de la Secretaría de Economía.
- Recomendaciones en Materia de Seguridad de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Conceptos Básicos

CONCEPTOS BÁSICOS

Antimalware

Programa o software que sirve para detectar, proteger y limpiar los dispositivos informáticos individuales y sistemas de tecnología de la información contra software malicioso como virus, software espía, gusanos, troyanos, piratas informáticos, ransomware y cryptojackers.

Aviso privacidad

Es un documento impreso, electrónico o en cualquier otro formato generado por el responsable (albergue) en el que se informa de manera sencilla, con un lenguaje claro y comprensible, el alcance, términos y condiciones del tratamiento que se dará a los datos personales, es decir explica quién y qué datos recaba, para qué y cómo los utiliza, de manera que el titular pueda tomar una decisión informada sobre el uso de sus datos, a efecto de mantener el control y disposición sobre ellos. De acuerdo con los Lineamientos del Aviso de Privacidad existen tres modalidades de aviso de privacidad: integral, simplificado y corto.

Aviso corto

Se utiliza cuando el espacio utilizado para la obtención de los datos personales sea mínimo y limitado, de manera que la información personal recabada o el espacio para la difusión o reproducción del aviso de privacidad también lo sean, por ejemplo, se puede usar en mensajes SMS, listas de asistencia o de registro de personas. Según los Lineamientos del Aviso de Privacidad el contenido a informar comprende: 1) la identidad y domicilio del responsable; 2) las finalidades primarias del tratamiento; y 3) los mecanismos para que el titular conozca el aviso de privacidad integral.

Aviso privacidad integral

Es el aviso de privacidad más completo, se usa cuando los datos se recaban personalmente del titular con presencia física. De acuerdo con los Lineamientos del Aviso de Privacidad el contenido a informar comprende: 1) la identidad y domicilio del responsable (albergue); 2) las finalidades primarias y secundarias del tratamiento; 3) los mecanismos para que el titular pueda manifestar su negativa para finalidades secundarias o accesorias; 4) los datos personales tratados; 5) el señalamiento expreso de los datos personales sensibles que se traten; 6) las transferencias de datos personales que en su caso se efectúen; 7) la cláusula que indique si el titular acepta o no la transferencia cuando así se requiera; 8) los medios y el procedimiento para ejercer los derechos ARCO; 9) los mecanismos y procedimientos para que, en su caso, el titular pueda revocar su consentimiento al tratamiento de sus datos personales; 10) las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de sus datos personales; 11) el uso de cookies, web beacons o cualquier otra tecnología similar o análoga; y 12) los procedimientos y medios por los cuales el responsable comunicará a los titulares los cambios en el aviso de privacidad.

Aviso privacidad simplificado

Se utiliza cuando los datos personales se obtienen de manera directa del titular a través del Internet o vía telefónica. De acuerdo con los Lineamientos del Aviso de Privacidad el contenido a informar comprende: 1) la identidad y domicilio del responsable; 2) las finalidades primarias del tratamiento; 3) los mecanismos para que el titular pueda manifestar previamente su negativa para el tratamiento de sus datos personales respecto de aquellas finalidades secundarias o accesorias, y 4) los mecanismos para que el titular conozca el aviso de privacidad integral.

Confidencialidad

Este deber implica la obligación de guardar secreto respecto de los datos personales que son tratados, es necesario su cumplimiento para evitar causar daño al titular. El responsable debe adoptar medidas para evitar que un tercero no autorizado acceda a los datos y para que quienes tengan autorización no divulguen dicha información.

Consentimiento

Es la manifestación libre e informada de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de estos. El consentimiento puede ser: a) tácito que es aquel que se otorga cuando el titular no niega que sus datos personales sean tratados después de haber conocido el aviso de privacidad; b) expreso, que se requiere para el manejo de datos financieros, patrimoniales y sensibles y exige que se facilite al titular un medio sencillo y gratuito para manifestarlo; o c) escrito, el cual se otorga cuando el titular lo externa mediante firma autógrafa o electrónica o huella dactilar o cualquier mecanismo autorizado, se utiliza en los mismos casos que el consentimiento expreso.

Conservación

Los plazos de conservación de los datos personales no deben de exceder aquellos que sean necesarios para el cumplimiento de las finalidades que justificaron el tratamiento. Una vez cumplida la finalidad deberá proceder la cancelación de los datos.

Datos patrimoniales o financieros

Información concerniente a una persona física relativa a sus bienes, derechos u obligaciones susceptibles de valoración económica, como pueden ser: bienes muebles e inmuebles; información fiscal; historial crediticio; ingresos y egresos; cuentas bancarias; seguros; afores; fianzas, número de tarjeta de crédito, número de seguridad, entre otros.

Datos personales

Cualquier información concerniente a una persona física, que la identifique o que la haga identificable, expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o en cualquier tipo, tales como nombre, nivel de estudios, domicilio, número de pasaporte, correo electrónico, etc.

Datos sensibles

Son aquellos datos personales que afectan la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para la persona, por ejemplo: origen étnico o racial; estado de salud pasado, presente o futuro; información genética; creencias religiosas, filosóficas y morales; estatus migratorio, afiliación sindical; opiniones políticas; preferencia sexual y/o necesidades de servicios especializados como servicios jurídicos, psiquiátricos, entre otros.

Derecho a la autodeterminación informativa

El poder de las personas de decidir quién puede tratar sus datos y para qué fines. Así mismo, da la facultad a las personas para disponer de la información que tienen sobre sí las instituciones en sus registros o bases de datos.

Derechos ARCO

Son aquellos derechos que pueden ejercer los titulares para acceder, rectificar, cancelar y oponerse al tratamiento de sus datos personales. El titular puede presentar por sí mismo o por medio de un representante una solicitud ante el responsable para ejercer dichos derechos.

Derecho de Acceso

Es el derecho de los titulares a acceder a los datos personales en poder del responsable, conocer el aviso de privacidad al que está sujeto el tratamiento de sus datos. Se da por cumplido cuando el responsable ponga a disposición del titular los datos personales en sitio o mediante la expedición de copias simples u otros formatos previstos en el aviso de privacidad.

Derecho de Rectificación

Es el derecho de los titulares a rectificar sus datos personales cuando sean inexactos o incompletos. Deberá presentar una solicitud de rectificación en la que indique a qué datos se refiere y la corrección que debe realizarse. Se debe de acompañar con la documentación que ampare la procedencia de lo solicitado.

Derecho de Cancelación

Es el derecho de las titulares de solicitar en todo momento al responsable la cancelación de los datos personales cuando considere que los mismos no están siendo tratados conforme a los principios y deberes establecidos en la LFPDPPP y su reglamento. Se pueden cancelar la totalidad de los datos contenidos en la base de datos o solo parte de ellos, según lo solicite el titular. La cancelación dará paso a un periodo de bloqueo, después del cual se procederá a la suspensión del dato.

Derecho de Oposición

Es el derecho del titular a oponerse al tratamiento de sus datos o que cese en el mismo. De ser procedente la solicitud, el responsable no podrá tratar los datos relativos al titular. Se debe justificar que aun siendo lícito el tratamiento de sus datos personales, el mismo debe cesar para evitar que su persistencia cause un perjuicio al titular.

Derecho de Revocación

Además de los derechos ARCO, las personas pueden revocar el consentimiento al tratamiento de sus datos personales en cualquier momento, siempre que esto no lo impida una disposición legal. El responsable deberá establecer mecanismos sencillos y gratuitos para que el titular revoque su consentimiento, al menos por el mismo medio por el que lo otorgó. Existen dos modalidades de la revocación: a) sobre la totalidad de las finalidades consentidas; y b) la revocación parcial del consentimiento donde el titular mantiene el consentimiento para ciertos fines.

Derecho a la Privacidad

Es un derecho humano según el cual nadie debe ser objeto de injerencias, arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Disociación

Procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

Encargado

Es la persona física o jurídica ajena a la organización del responsable que, sola o conjuntamente con otras, trate datos personales por cuenta del responsable. El encargado no decide sobre el tratamiento de los datos personales, sino que lo realiza siguiendo las instrucciones del responsable. Debe de guardar la confidencialidad respecto de los datos personales tratados y tratar los datos únicamente conforme a las instrucciones del responsable.

Finalidad o finalidades del tratamiento

Se determina(n) cuando con claridad, sin lugar a confusión y de manera objetiva, se especifican los objetivos del tratamiento de datos personales.

Medidas de seguridad administrativas

Son las acciones y mecanismos para establecer la gestión, soporte y revisión la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal en materia de protección de datos personales.

Medidas de seguridad físicas

Acciones y mecanismos que empleen o no tecnología destinados a: a) prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información; b) proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones; c) proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad; y d) garantizar la eliminación de datos de forma segura.

Medidas de seguridad técnicas

Son las actividades, controles o mecanismos con resultado medible que se valen de la tecnología para asegurar que: a) el acceso a las bases de datos o a la información en formato lógico sea por usuarios identificados y autorizados; b) el acceso autorizado sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) se incluyan acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas de seguros; y d) se lleve a cabo la gestión de comunicaciones y operaciones de los recursos en el tratamiento de datos personales.

Política de escritorio limpio

Como el nombre lo indica es mantener el escritorio o área de trabajo limpia, lo cual implica no dejar documentos o información sensible, identificaciones o llaves a la vista de todos ni tener las contraseñas anotadas en un papel o Post-it. Las personas deben tener en su escritorio únicamente las cosas que necesitan para su día de trabajo y si van a dejar su escritorio para asistir a una reunión o tomar un descanso, deberán guardar los documentos físicos ya sea en un archivero o cajón y activar el protector de pantalla con contraseña de su computadora.

Principio de calidad

Se cumple cuando los datos que se traten sean exactos, completos, pertinentes, correctos y actualizados para la finalidad para la cual fueron recabados.

Principio de consentimiento

Todo tratamiento de datos personales deberá estar sujeto al consentimiento del titular, salvo en el caso de las excepciones que establece la ley. Debe cumplir con las siguientes características:

a) Ser libre, es decir que no medie error, mala fe, violencia o dolo que puedan afectar la manifestación de la voluntad del titular.
b) Ser específico, referido a una o varias finalidades determinadas que justifiquen el tratamiento.
c) Ser informado, que el titular tenga conocimiento del aviso de privacidad previo al tratamiento que serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento.

Principio de finalidad

El tratamiento de los datos personales deberá limitarse al cumplimiento de las finalidades para las cuales se haya obtenido, mismas que deben estar previstas en el aviso de privacidad.

Principio de información

Se refiere a la obligación del responsable de hacer saber a los titulares de los datos personales la información que se recaba de ellos, con que fines y el tratamiento que le dará a los datos, lo que se realizará a través del aviso de privacidad.

Principio de licitud

Se refiere a que los datos deberán recabarse y tratarse en apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional. Es decir, con pleno cumplimiento de la legalidad y respeto de la buena fe y los derechos del individuo, cuya información es sometida a tratamiento.

Principio de lealtad

Establece la obligación de que el tratamiento de los datos personales se realice en atención a lo acordado, tomando en consideración la expectativa razonable de privacidad del titular de los datos, sin causar perjuicio alguno a los intereses del titular. Lo anterior implica que la obtención o conservación de datos personales no se realice a través de medios engañosos o fraudulentos. Se considera que se actúa de manera fraudulenta cuando: a) exista dolo, mala fe o negligencia en la información proporcionada al titular respecto al tratamiento de datos personales, b) se vulnere la expectativa razonable de privacidad, c) las finalidades no fueron informadas en el aviso de privacidad.

Principio de proporcionalidad

Se refiere a que el tratamiento de los datos personales será el que resulte necesario, adecuado y relevante en atención a las finalidades previstas en el aviso de privacidad.

Principio de responsabilidad

El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentran bajo su custodia o posesión o por aquellos que haya comunicado a un encargado. Este principio implica que el responsable deberá rendir al titular en caso de incumplimiento, independientemente de quien realice el tratamiento. Para cumplir con esta obligación puede valerse de estándares, mejores prácticas internacionales, políticas internas, esquemas de autorregulación o cualquier mecanismo que considere adecuado para tales fines.

Protección de datos personales

Es la aplicación sistemática de medidas de salvaguardas institucionales, sean estas técnicas o físicas, que tengan como finalidad preservar el derecho a la privacidad con respecto a la captura, almacenaje, uso y divulgación de datos personales.

Responsable

Persona física o moral de carácter privado que decide sobre el tratamiento de los datos personales, para el caso de esta guía se refiere a los albergues o sus titulares ya que para el desarrollo de sus actividades son quienes recaban, utilizan, almacenan y transfieren los datos personales.

Tercero

Persona física o moral, nacional o extranjera distinta del titular o del responsable de los datos.

Titular

Persona física a quien corresponden los datos personales.

Transferencia

Toda comunicación de datos realizada a personas distintas del responsable o del encargado. No deberá de realizarse ninguna transferencia sin el consentimiento del titular.

Tratamiento

La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Medidas para la Protección de Datos Personales

Mediante la adopción de políticas y programas de protección de **datos personales**, los albergues toman medidas institucionales cuya finalidad es preservar el derecho a la privacidad con respecto a la obtención, conservación, uso y **transferencia** de datos personales de personas migrantes, previniendo y minimizando riesgos de protección que enfrentan diferentes categorías de población migrante; entre ellos, extorsión, amenazas, discriminación y secuestro.

Toda política y programa de protección de **datos personales** deberá de observar los principios de licitud, lealtad, consentimiento, finalidad, proporcionalidad, calidad, información y responsabilidad señalados por la LFPDPPP y su reglamento. Así mismo, deberán ser compartidas con todo el personal y ejecutadas por las personas que tratan datos personales en los albergues.

1 DESIGNAR UNA PERSONA O DEPARTAMENTO DE DATOS PERSONALES

El albergue deberá designar a una persona o departamento dentro del albergue, o de serle conveniente una persona encargada[3] ajena a la organización, quien tendrá la función de fomentar la protección de **datos personales** y atender las solicitudes de las personas migrantes respecto a sus derechos en la materia.

Entre las actividades que llevará a cabo la persona o departamento de datos personales, se encuentran:

- Diseñar, difundir y ejecutar una política de protección de **datos personales** a partir de un diagnóstico y mapeo sobre los procesos internos de obtención, uso, conservación, **transferencia** y eliminación de los datos personales.
- Capacitar a las diferentes áreas del albergue sobre la política y la protección de **datos personales**.
- Crear un mecanismo de monitoreo y evaluación de las políticas a fin de asegurar su validez y efectividad.
- Establecer procedimientos para recibir, atender y dar seguimiento oportuno a las solicitudes de las personas migrantes sobre sus derechos de acceso, rectificación, cancelación u oposición sobre el **tratamiento** de sus **datos personales** (derechos ARCO) y de revocación del consentimiento[4].
- Recibir y atender las quejas relacionadas con las prácticas o políticas de protección de datos de la organización.

[3] Las personas encargadas son aquellas externas al albergue que manejan datos de las personas migrantes porque fueron contratadas para este fin. Para más información revisar la definición de cada derecho en la sección de Conceptos Básicos de la presente guía.
[4] Para más información revisar la definición de cada derecho en la sección de Conceptos Básicos de la presente guía.

La designación de la persona o departamento o del encargado dependerá del tipo y la cantidad de datos personales que maneje el albergue, así como del potencial de solicitudes que pueda recibir por parte las personas migrantes respecto a sus derechos de protección de datos.

Si bien no es necesario que la persona o departamento de datos personales se dedique únicamente a la protección de datos personales, deberá de tener conocimiento en la materia.

Es importante señalar que para el caso de que exista un encargado que trate por cuenta del responsable los **datos personales**, deberá de contar con cláusulas contractuales que permitan acreditar la existencia de la relación, su alcance y contenido, además del tratamiento que deberá de dar el encargado en seguimiento a las instrucciones brindadas por el responsable.

Recursos

Para determinar el perfil y las funciones de la persona o departamento de datos personales en el albergue puede revisar las *"Recomendaciones para la designación de la persona o departamento de datos personales"* del INAI en: http://inicio.inai.org.mx/DocumentosdeInteres/RecomendacionesDesignar.pdf.

2 ELABORAR UN DIAGNÓSTICO Y MAPEO

Antes de implementar un programa o política, el albergue debe de elaborar un diagnóstico y mapeo del tipo de dato personal que está recolectando, con qué fines, de quiénes, cómo se obtienen y se manejan los mismos.

Para identificar los tipos de **datos personales** que se están colectando es fundamental conocer la diferencia entre los datos personales y los datos sensibles. Los datos personales son cualquier información concerniente a una persona física que la identifique o la haga identificable expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o en cualquier tipo, ejemplos de ellos son el nombre, grado de estudios, domicilio, cédula profesional, correo electrónico, número de seguro social, etc. Por su parte, los datos sensibles son los datos personales que afectan la esfera más

íntima de su titular o cuya utilización indebida puede dar origen a actos discriminatorios o conlleve un riesgo grave para la persona. Se consideran datos sensibles: el origen étnico o racial, el estado de salud, la información genética, las creencias religiosas, filosóficas y morales, la afiliación sindical, el estatus migratorio, las opiniones políticas, las preferencias sexuales y/o las necesidades de servicios especializados como servicios jurídicos, psiquiátricos, entre otros.

Es importante revisar que en el albergue se están recabando solamente los datos personales y sensibles mínimos necesarios, adecuados y relevantes para dar cumplimiento a las actividades relacionadas con el albergue, ya que entre más datos se recolectan se aumentan los riesgos en su tratamiento.

Además, se debe evaluar el riesgo inherente que tienen los datos personales y/o sensibles que se tratan, midiendo el valor que tienen para los titulares, los responsables y las personas no autorizadas que pudieran beneficiarse de ellos. Se pueden clasificar los niveles de riesgo o sensibilidad de los datos como:

a) Nivel estándar o con riesgo inherente bajo, que normalmente incluye información de identificación, de contacto, laborales y académicos (nombre, teléfono, edad, estado civil, grado de estudio, nacionalidad, puesto de trabajo, idioma, etc.).
b) Nivel sensible o con riesgo inherente medio que incluye datos que permiten conocer la ubicación física, inferir el patrimonio, autenticación, datos que se estén usando en procesos jurídicos o aquellos que afecten la esfera más íntima de las personas (dirección física, saldos bancarios, estados de cuenta, antecedentes penales, demandas, huellas dactilares, firma autógrafa, afiliación religiosa, estado de salud, preferencia sexual, etc.).
c) Nivel especial o con riesgo inherente alto que son los datos cuya naturaleza única puede causar daño directo a las personas mencionado en combinación con cualquier otro dato relacionado o contenido en la misma (número de tarjeta bancaria y código de seguridad).

Se debe de valorar si el tratamiento que se está otorgando corresponde a las finalidades consentidas por el titular y si se está obteniendo el consentimiento expreso y/o por escrito sobre los datos personales que dispone la ley.

A continuación, se presenta una tabla que puede ayudar a realizar el mapeo de los datos personales y su manejo por parte del albergue.

Tabla de mapeo de datos personales

Manejo de datos	Sí	¿Quién (es) los manejan?	No
¿La organización recaba datos personales?			
¿La organización usa datos personales?			
¿La organización almacena datos personales?			
¿La organización borra datos personales?			
¿La organización recaba datos sensibles?			
¿La organización usa datos sensibles?			
¿La organización almacena datos sensibles?			
¿La organización borra datos sensibles?			

Tipos de Datos personales/sensibles	¿Ya se recaba? Sí	No	Necesario Sí	No	Tipo de sensibilidad o nivel de riesgo inherente
Nombre					
Edad					
Sexo					
Correo					
Teléfono					
Estado civil					
Domicilio					
Firma					

Datos personales sensibles	Sí	No	Sí	No	Tipo de sensibilidad o nivel de riesgo inherente
Religión					
Estado de salud					
Orientación sexual					
Identidad de género					
Pertenencia a grupo étnico					
Estatus migratorio					
Víctima de delito					
Antecedentes penales					
Situación jurídica					
Razones de proyecto migratorio					

Tabla de mapeo de datos personales

Formato de obtención de datos personales	Físico	Digital	Personas/áreas con acceso
(Ejemplos) Entrevista de personas			
Correos electrónicos			
Listas de registro entradas/salidas albergue			
Bases de datos			
Pertenencia a grupo étnico			
Copias de documentos de identidad (pasaporte, CURP, etc.)			
Expedientes			

También, se debe identificar con quiénes se comparten los datos fuera de la organización (terceros[5] y/o encargados[6]), el propósito de esta transferencia, cómo se almacenan los datos, por cuánto tiempo y cuáles son los procesos para la eliminación de estos datos. Para ello puede hacer uso de la tabla que se presenta a continuación:

Tabla mapeo almacenamiento y transferencia de datos

¿De quién se obtiene los datos personales?	¿Qué área maneja sus datos?	¿Cuál es el motivo del manejo de sus datos?	¿Por cuánto tiempo almacenan los datos?	¿Se comparten estos datos con externos al albergue?	¿Con quiénes se comparten y por qué?
(Ejemplos) Personas migrantes					
Asistentes talleres					
Voluntarios					
Personal					
Trabajadores sociales					

[5] Por ejemplo: financiadoras, instancias de gobierno o de sociedad civil que brindan servicios a las personas migrantes, etc.
[6] Por ejemplo: empresas subcontratadas para el manejo de la nómina, call centers, empresas que manejan datos en la nube o que se encargan de destrucción de datos.

Es importante evaluar la necesidad de compartir datos personales con terceros o si es mejor compartir los datos como agregados anónimos para análisis estadísticos o hacerlos pasar por un método de disociación[7] de manera que no se puedan relacionar con el titular. Entre los métodos más comunes para eliminar los factores identificables y preservar la confidencialidad y el anonimato de las personas se encuentran:

a) **La codificación de datos.** Consiste en reemplazar la identidad de los titulares y otros datos que sean identificables por etiquetas, números o letras no conectados para evitar su identificación. Este mecanismo es útil para el manejo de grandes bases de datos. Por ejemplo: cuando se recaba el estado de salud de las personas, asignar en la sección correspondiente de la base de datos las letras AK para identificar a personas con VIH y la letra B F para personas con problemas de adicción. Se recomienda que las claves o contraseñas que permiten decodificar el conjunto de datos, se almacenen de forma segura por el personal autorizado del albergue.

b) **La seudonimización.** Es un proceso mediante el cual se sustituye información personal por uno o más identificadores artificiales o seudónimos de manera que hace que la persona no sea identificable. Se sugiere adoptar esta práctica para reportar estudios de caso o reportes para donantes. Para explicar un caso paradigmático se puede usar solo el sexo de la persona (refiriéndose a un hombre o una mujer) o cambiar su nombre, usar una nacionalidad distinta o inventada y cambiar la edad de manera que no sea posible reconocer la persona que fue víctima de un delito u otra circunstancia sensible. Por ejemplo: Juan de 20 años es del país Verde, se acercó al albergue porque fue víctima de secuestro en su trayecto por México, gracias a nuestra gestión, Juan pudo interponer una denuncia ante el organismo correspondiente, obtener la tarjeta de visitante por razones humanitarias y quedar fuera de peligro.

c) **La anonimización.** Es un proceso que suprime aquella información que permite identificar a una persona. Por ejemplo: eliminar los nombres de las personas, la dirección y dejar las edades en las bases de datos. Se puede combinar con la seudominización y codificación de datos, quedando una base donde se supriman los nombres, se empleen claves para la condición de salud y se dejen el sexo, la edad y nacionalidad de las personas.

Recursos

Para el recurso completo de mapeo de datos personales puede tomar como referencia el Anexo 1. *Mapeo de datos personales* y *diagnóstico de protección de datos personales* disponible en la pág. 41 de la presente guía.

3 ELABORAR UNA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Para la elaboración de una política de protección de datos es fundamental determinar roles y responsabilidades de las diferentes áreas del albergue respecto a la obtención, uso, conservación, **transferencia** y eliminación de los **datos personales** de las personas migrantes.

Dicha política deberá de observar los principios de protección de datos personales previstos en la LFPDPPP en cada una de las fases del ciclo de vida de los datos, a la vez que da cumplimiento a los deberes de seguridad y confidencialidad.

Diagrama cumplimiento de principios y deberes en el ciclo de vida de los datos

[7] Para más información revisar la definición de cada derecho en la sección de Conceptos Básicos de la presente guía.

Fase 1

Se deberán implementar políticas que establezcan únicamente la recolección de datos mínimos necesarios y de los cuales se haya obtenido el consentimiento, respetando la ley, sin utilizar medios engañosos e informando al titular sobre cómo serán tratados. Al mismo tiempo, se procurarán políticas para que los datos obtenidos sean exactos, completos y correctos. La confidencialidad deberá ser respetada durante todo el proceso de obtención de datos.

Fase 2

Se deben diseñar acciones que limiten el uso de los datos personales a las finalidades consentidas por el titular, debiéndose adoptar las medidas necesarias que garanticen la integridad, confidencialidad y disponibilidad de los datos. En todo momento, se debe evitar la alteración, pérdida, transmisión y acceso no autorizado, ya sea durante su uso o almacenamiento, de manera que no se trasgreda la confianza que depositó la persona migrante en el albergue.

Fase 3

En caso de que existan transferencias a terceros, se deberán implementar políticas para informar y obtener el consentimiento de los titulares sobre estos procesos y para que los terceros conozcan y cumplan con las finalidades autorizadas para el tratamiento de los datos transferidos.

Fase 4

Los datos personales podrán conservarse hasta que cumplan con la finalidad o propósito para el cual fueron obtenidos, por lo que se deben generar políticas que establezcan los periodos de conservación, así como los mecanismos que se utilizarán para su correcta eliminación, borrado o destrucción.

Así mismo, se deberán establecer políticas y mecanismos para que las personas migrantes tengan acceso a sus derechos ARCO.

Derechos ARCO

Todas las personas tienen el derecho de Acceder, Rectificar, Cancelar y Oponerse sobre sus datos, lo que se conoce como derechos ARCO[8], por lo que el albergue tiene la obligación de establecer un mecanismo de acceso a estos y de responder a todas las solicitudes de acceso que se presenten sin importar el sentido de su respuesta.

El titular o su representante deberán presentar una solicitud para ejercer sus derechos en dicho mecanismo la cual, según la LFPDPPP, deberá tener el nombre del titular y el domicilio o medio para ser contactado, descripción clara y precisa de los datos personales de los que quiere ejercer sus derechos y elementos que faciliten su localización. Así mismo el titular deberá presentar un documento que acredite su identidad (pasaporte, documento de identidad, documento migratorio, constancia de residencia, constancia de origen, etc.) o, en su caso, la representación legal del titular (carta poder o declaración de competencia). El albergue deberá de emitir un acuse de recibido con la fecha de recepción de la solicitud.

Se recomienda que la persona o el departamento de datos personales designado por el albergue disponga de una cuenta de correo electrónico exclusiva para recibir las solicitudes de acceso a los derechos ARCO, mismo que deberá aparecer en el **aviso de privacidad**. En caso de no contar con comunicaciones por esta vía, se deberá compartir la dirección física a la cual las personas pueden entregar sus solicitudes.

La LFPDPPP y su reglamento establecen plazos para las respuestas a las solicitudes por lo que se sugiere contar con lineamientos internos para dar cumplimiento en la materia.

Si la solicitud no es clara, está incompleta o es errónea el albergue puede solicitar al titular información adicional dentro de los siguientes 5 días después de recibida la solicitud. El titular tiene 10 días para atender al requerimiento, en caso de no dar respuesta se tendrá por no presentada.

Si la solicitud está completa y es clara, el albergue tiene un plazo máximo de 20 días contados a partir de la fecha en que se recibió la solicitud de acceso, rectificación, cancelación u oposición para comunicar al titular si la solicitud resulta procedente o no. En caso de no poder cumplir dicho plazo, se puede ampliar por una sola ocasión de manera justificada por 20 días más, lo cual deberá de notificarse al titular.

[8] El art. 28 de la LFPDPPP establece que el titular o su representante legal podrán solicitar al responsable en cualquier momento el acceso, rectificación, cancelación u oposición, respecto de los datos personales que le conciernen.

Una solicitud no es procedente cuando:

a) El solicitante no es el titular de los datos personales o el representante no esté debidamente acreditado.
b) No se encuentren los datos personales en las bases de datos del albergue.
c) Se lesionen los derechos de terceros.
d) Exista un impedimento legal o una resolución de una autoridad competente que restrinja el acceso a los datos o no permita su rectificación, cancelación u oposición.
e) La rectificación, cancelación u oposición haya sido realizada previamente.

Si la solicitud no es procedente, el albergue deberá comunicarlo al titular, explicando el motivo de su decisión por el mismo medio en el que se llevó a cabo la solicitud, acompañado de las pruebas que considere pertinentes.

En caso de que la solicitud sea procedente, deberá hacerse efectivo su derecho ARCO, para lo cual el albergue tiene 15 días a partir de la respuesta de la procedencia para atender a la petición del titular, teniendo la posibilidad de ampliarlo solo por una ocasión de manera justificada por el mismo número de días.

El ejercicio de los derechos debe ser sencillo y gratuito, por lo que el titular solo cubrirá gastos de envío, reproducción y certificación de documentos (si procede). La respuesta tendrá que referirse a los datos personales indicados en la solicitud y se debe de presentar en un formato legible, comprensible y de fácil acceso.

Es importante señalar que si el albergue no da respuesta o si el titular no está conforme con lo respondido podrá iniciarse un procedimiento de tutela o de protección de derechos frente al INAI.

4 CONTAR CON UN AVISO DE PRIVACIDAD

La LFPDPPP establece la obligación de que el albergue como responsable del tratamiento de los datos elabore y ponga a disposición de las personas migrantes un **aviso de privacidad**. El **aviso de privacidad** es un documento físico, electrónico o en cualquier formato por medio del cual se informa a las personas sobre los datos que el albergue está recabando sobre ellas y los usos que dará a la información. El aviso de privacidad deberá contener como mínimo:

- Nombre y domicilio del albergue que lo recaba.
- Finalidades del **tratamiento** de los datos.
- Opciones y medios que se ofrecen para limitar el uso de divulgación de los datos.
- Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición.
- Si se compartirán los datos con terceros, en qué condiciones, a quiénes será y con qué finalidad.

Se recomienda retomar los resultados del diagnóstico o mapeo para la redacción del **aviso de privacidad**.

Adicionalmente, es relevante tener presente los perfiles de los titulares al momento de redactar el aviso de privacidad, con la intención de que la redacción sea clara, sencilla, en el idioma de la persona migrante y conforme al público objetivo, de manera que no genere confusiones.

De acuerdo con los Lineamientos del aviso de privacidad existen tres modalidades del **aviso de privacidad**: integral, simplificado y corto[9], los cuales tienen diferentes contenidos y reglas de aplicación según la manera en que se recaban los datos personales.

Dado que los albergues obtienen datos personales en presencia de las personas migrantes, se debe contar con el **aviso de privacidad** integral, debiéndose entregar una copia impresa a las personas antes de recabar los datos o difundir su contenido por medio de un cartel visible.

Si el albergue obtiene los datos de las personas por internet (página de internet, Facebook, correo electrónico) o por teléfono, puede usar el **aviso de privacidad** simplificado; dando a conocer este formato en su página de internet, en la parte inferior del correo electrónico o por medio de una grabación sonora en su teléfono.

[9] Para más información sobre sus usos, revisar la sección de Conceptos Básicos de la presente guía.

Existen diferentes medios para dar a conocer el **aviso de privacidad** y usted puede utilizar el medio que considere más conveniente, siempre y cuando esté ubicado en un lugar visible que facilite su consulta.

Ejemplo de Aviso de Privacidad

Aviso de Privacidad

El Albergue la Vía con domicilio en Avenida del Libro#2, Col. Ciencias, Ciudad de México, C.P. 12345, es el responsable del uso y protección de sus datos personales. Los datos personales que recabamos son:

- Nombre completo, estado civil, lugar y fecha de nacimiento, nacionalidad, teléfono, datos de contacto en caso de una emergencia, datos sobre su condición migratoria y firma autógrafa.

Adicionalmente se pueden recabar algunos datos sensibles como son:

- Datos sobre su estado de salud física o mental, datos sobre si ha sido víctima de algún delito, datos sobre antecedentes penales, datos sobre sus opiniones políticas y creencias religiosas.

Los datos arriba señalados se utilizarán para las siguientes finalidades que son necesarias para otorgar nuestros servicios:

a) Registro de entrada y salida de las instalaciones
b) Para la integración de su expediente, brindar información y orientación
c) Para brindar asistencia médica y psicológica

De manera adicional, utilizaremos su información personal para las siguientes finalidades que no son necesarias para el servicio solicitado, pero que nos permiten y facilitan brindarle una mejor atención:

a) Avisar a sus familiares o consulado en caso de algún accidente o que no sea posible localizarle.

En caso de que no desee que sus datos personales se utilicen para estos fines, indíquelo a continuación:

☐ No consiento que mis datos personales se utilicen para avisar a mis familiares o consulado en caso de algún accidente o que no sea posible localizarme.

Le informamos que sus datos personales son compartidos con las siguientes organizaciones y autoridades distintas a nosotros, para los fines que se presentan a continuación, favor de indicar con una X si autoriza o no la transferencia con dichas instituciones.

Organización	Finalidad	Otorga su consentimiento	
Fiscalía del Estado	Acompañamiento y presentación de denuncias, apertura de carpetas de investigación	Sí	No
Instituto de la defensoría pública	Representación jurídica	Sí	No
Centros y clínicas de salud	Atención médica	Sí	No
Albergue El Pastor	Canalización a servicios del albergue	Sí	No

Puede ejercer su derecho a acceder, rectificar, cancelar u oponerse sobre sus datos y para revocar el consentimiento al tratamiento de sus datos en los casos que sean aplicables enviando su solicitud al correo: alavia@mail.com o poniéndose en contacto con el departamento de protección de datos personales quien atenderá a sus solicitudes y dudas respecto al tema en: en Avenida del Libro#2, Col. Ciencias, Ciudad de México, C.P. 12345, tel. 55 12345678 ext. 910

En caso de realizar alguna modificación al Aviso de Privacidad, se le hará de su conocimiento vía correo electrónico o bien, a través del portal de nuestra página de internet: www.alberguelavia.org.

Consiento que mis datos personales y sensibles sean tratados conforme a los términos y condiciones del presente Aviso de Privacidad

_____ _____

Nombre del titular Firma del titular

_____

Lugar y fecha

Fecha de actualización al presente aviso de privacidad: noviembre de 2019

Recursos

Para más información sobre cómo elaborar el aviso de privacidad puede revisar *El ABC del Aviso de Privacidad* del INAI en: http://abcavisosprivacidad.ifai.org.mx/. También puede elaborar su aviso de privacidad por medio del servicio gratuito en línea del INAI *Generador de Avisos de Privacidad Sector Privado* disponible en: http://generador-avisos-privacidad.inai.org.mx/users/login.

Puede tomar como referencia el Anexo 2. Ejemplos de *Avisos de Privacidad Modelo para Albergues* disponible en la pág. 47 de la presente guía.

5 OBTENER EL CONSENTIMIENTO

Para el **tratamiento** y la **transferencia** de **datos personales a terceros**[10], tales como instancias de servicios a donde se canalizan a las personas, es necesario solicitar el consentimiento libre e informado de las personas migrantes por lo que deben de conocer y entender el **aviso de privacidad** antes de que proporcionen sus datos. La solicitud del consentimiento deberá ir ligada con las finalidades específicas del **tratamiento** establecidas en el **aviso de privacidad**.

El formato de consentimiento puede estar incluido dentro del aviso de privacidad mediante la inclusión de casillas o deberá estar a disposición por otro medio que sea sencillo y gratuito de manera que el titular pueda manifestar su autorización o negativa sobre el tratamiento y/o transferencia de sus datos.

Si se trata de niñas, niños o adolescentes, aunque se debe considerar su punto de vista y opinión en todo momento, se deberá evaluar si comprende los riesgos y los beneficios involucrados del uso y transferencia de sus datos, en correspondencia con su edad y madurez. Si no tiene la capacidad legal para consentir, se deberá de obtener el consentimiento por parte de alguno de sus padres, tutor o quien ejerza la patria potestad y representación legal, quienes deberán estar claramente informados.

[10] Las personas o instituciones que reciban los datos deben de tratar los datos como lo establece el aviso de privacidad del albergue, por lo que se deben de compartir las condiciones en las que las personas consintieron el tratamiento de sus datos, ya sea por medio de compartir el aviso de privacidad con los terceros, cláusulas contractuales u otros instrumentos jurídicos.

En caso de que la persona no proporcione su consentimiento, deberá ser informada sobre las implicaciones y efectos que puede tener sobre la prestación de servicios y no se obtendrán sus datos personales.

Cuando personal del albergue, o de otra organización, tome fotografías[11], videos o audio de las personas migrantes alojadas para la documentación y promoción de las actividades que realiza, se recomienda contar con un consentimiento específico explicando las finalidades de su tratamiento. Tome en cuenta que una vez que una fotografía o video se publique en redes sociales será difícil de eliminar todas las copias por lo que es importante cerciorarse que las personas que participen en este tipo de difusión no se expongan a un mayor riesgo, como podría ser el caso de víctimas de trata, de delitos en territorio mexicano, de violencia basada en género, solicitantes del reconocimiento de la condición de refugiado, entre otros.

Revocación de Consentimiento

El consentimiento no es estático y puede ser revocado en cualquier momento que las personas lo deseen, es por ello la importancia de contar con un mecanismo sencillo y gratuito para responder a este tipo de solicitud y realizar la revocación y la eliminación de dichos datos personales.

Para solicitar la revocación del consentimiento la persona tendrá que indicar al responsable si la revocación será parcial (se cesa el tratamiento de algunos datos) o total (se cesa el tratamiento de todos los datos). En caso de ser una revocación parcial deberá indicar los tratamientos con los que no está conforme.

Para este proceso, el albergue tendrá que cumplir y dar respuesta en los mismos plazos establecidos para los derechos ARCO y debe de otorgar una confirmación del cese del tratamiento de los datos personales al titular. Si los datos personales fueron compartidos con terceros o con un encargado, el albergue deberá de comunicarles la solicitud de revocación para que también cesen el tratamiento de éstos.

[11] Puede tomar como referencia el Anexo 3. Formato de Consentimiento para tomar fotografías, videos o audio de personas migrantes disponible en la pág. 54 de la presente guía.

Existen algunas excepciones sobre la aplicación de la revocación, las cuales se dan cuando el tratamiento sea necesario por:

a) Cumplir un contrato.
b) Una disposición legal.
c) Formar parte de actuaciones jurídicas.
d) Sea parte de un juicio.
e) Protección de los intereses del particular.
f) Ser considerado de interés público.
g) Relacionarse con la salud del titular.

Transferencia de datos

En caso de compartir **datos personales** con terceros, éstos deben de limitarse a las finalidades y a las condiciones establecidas en el **aviso de privacidad** y deberán realizarse tomando las medidas de seguridad necesarias para su protección. Es importante mantener un registro sobre la transferencia de los datos a terceros, donde se incluya el nombre del tercero, el propósito por el cual se realizó la transferencia, la fecha de la transferencia y una breve descripción de la categoría de datos transferidos.

Se puede tomar como referencia la tabla de Registro de transferencias a terceros presentada a continuación:

Nombre de la instancia a quien se comparten los datos	Nombre, teléfono y correo electrónico de la persona que recibe los datos personales	Datos transferidos y finalidades Fecha

Excepciones

De acuerdo con el artículo 37 de la LFPDPPP, existen algunos supuestos en los que no se requiere del consentimiento de las personas para la transferencia de sus datos a terceros, se resaltan los siguientes:

a) Cuando la transferencia esté prevista en una Ley mexicana vigente. Para estos casos, si una dependencia de gobierno solicita los datos, deberá de hacerlo mediante oficio, fundando y motivando su solicitud, enmarcando claramente cuáles son las leyes y los artículos que soportan que se transfieran los datos personales.

b) Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios.
c) Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas. Por ejemplo, cuando un ONG administra varios albergues u oficinas en diferentes puntos geográficos, se pueden transferir datos entre ellas sin requerir el consentimiento del titular. Esto no aplica si el albergue quisiera transferir datos con actores que formen parte de una misma red colaborativa, dado que son terceros, es decir, ajenos a la organización. Para este último escenario, siempre será necesario contar con el consentimiento de la persona migrante.
d) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia.
e) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
f) Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

Para los casos de procuración o administración de justicia o para el reconocimiento, ejercicio o defensa de un proceso judicial, la autoridad deberá mostrar una orden, mandato o resolución judicial debidamente fundada y motivada[12] sobre la causa legal del procedimiento. Este tipo de documentos son emitidos únicamente por un juez. Si no son presentados por la institución pública que solicita los datos, no deberá de proceder la transferencia.

El Instituto Nacional de Migración es la única autoridad con la facultad para realizar verificaciones migratorias y comprobar que las personas que se encuentran en territorio nacional cumplen con las obligaciones previstas en la Ley de Migración y su reglamento, si bien hay otras autoridades que pueden colaborar con el Instituto para el ejercicio de sus funciones, como la Policía Federal o la Guardia Nacional, esto no implica que puedan realizar funciones de verificación de forma independiente[13].

Las verificaciones migratorias no forman parte de los supuestos de excepción de consentimiento de transferencia de datos personales y, según el art. 76 de la Ley de

[12] De acuerdo con el artículo 16 de la CPEUM todo acto de autoridad debe estar fundado y motivado. Se entiende por fundado que ha de expresarse con precisión la ley aplicable al caso y, por motivado que deben señalarse, con precisión, las circunstancias especiales, razones particulares o causas inmediatas que se hayan tenido en consideración para la emisión del acto.
[13] Art. 96 de la Ley de Migración.

Migración, el Instituto Nacional de Migración no puede realizar verificaciones migratorias en los espacios de las organizaciones de la sociedad civil (las cuales deben de estar legalmente constituidas según lo establece el reglamento de la citada ley) o de las personas que realizan actos humanitarios o de protección en los que se encuentran albergadas las personas migrantes por lo que no se deberán de compartir los datos personales con este organismo sin el consentimiento previo del titular.

Por otro lado, si el albergue recibe solicitudes de reportes sobre las personas migrantes beneficiarias de sus servicios por parte de instituciones de financiamiento y/o donantes, sean estos gubernamentales o no, solo podrá compartir información en formato estadístico sin revelar los datos personales.

6 GUARDAR LA CONFIDENCIALIDAD

El albergue es responsable de guardar secreto sobre los datos personales de las personas migrantes en cualquier fase del **tratamiento** de los datos, incluso después de finalizar la relación con el **titular**. Esto lo debe hacer por medio de la adopción de medidas que eviten a personas no autorizadas el acceso a determinada información o una divulgación inapropiada por parte de personas autorizadas, independientemente que se concretice un perjuicio o no a la persona migrante.

Por ejemplo, se puede instaurar una política o lineamiento que dicte que la obtención de datos sensibles se realice únicamente en espacios privados y seguros en los que se garantice la privacidad, determinando que solo personas autorizadas pueden solicitar este tipo de información lo que puede aplicarse en la realización de entrevistas de ingreso al albergue o para el seguimiento de casos jurídicos.

Los albergues deben establecer procedimientos que eviten la fuga de información o el acceso indebido a los datos personales de migrantes e incluir cláusulas de confidencialidad en los contratos o instrumentos que celebre con terceros. Se sugiere usar herramientas como una carta compromiso de confidencialidad que firmen tanto el personal del albergue como los voluntarios de manera que todas las personas con las que trabaja el albergue se involucren en cuidar los datos personales[14]. También para el manejo y almacenamiento de documentos impresos con datos sensibles o personales, se pueden usar archiveros o gabinetes con cerraduras o cuartos con acceso restringido. Un aspecto complementario importante es incorporar actividades de capacitación al personal sobre sus obligaciones con relación al **tratamiento** de los **datos personales**.

[14] Puede tomar como referencia el Anexo 4. Formato de Carta compromiso de confidencialidad disponible en la pág. 55 de la presente guía.

Recursos

Puede tomar como referencia el Anexo 4. *Formato de Carta compromiso de confidencialidad* disponible en la pág. 55 de la presente guía.

7 ESTABLECER MEDIDAS DE SEGURIDAD

Los datos personales están expuestos a diferentes amenazas a lo largo de su tratamiento, esto puede ser ya sea porque una persona no autorizada quiera engañar al personal y robar los datos por medio de un *malware*, que en un descuido se perdió la *USB* con los expedientes del albergue o por un evento fortuito como el que por una inundación en el albergue dejen de funcionar los equipos de cómputo.

En ese sentido, el reglamento de la LFPDPPP establece cuatro tipos de vulneraciones de seguridad a los que pueden enfrentar los datos personales en cualquier etapa de su tratamiento:

a) Robo, extravío o que se realice copia no autorizada.
b) Pérdida o destrucción no autorizada.
c) Uso o acceso no autorizado.
d) Daño, alteración o modificación no autorizada.

La LFPDPPP y su reglamento establecen la obligación de la aplicación sistemática de medidas de seguridad administrativas, técnicas y físicas[15] que permitan garantizar el ejercicio y goce de los derechos a la protección de datos, la autodeterminación informativa, la integridad y la seguridad de las personas migrantes. Esto se puede realizar a través de un Sistema de Gestión de Seguridad de Datos Personales como lo establece la recomendación general del INAI[16].

[15] Para más información sobre los diferentes tipos de medidas de seguridad, revisar la sección de Conceptos Básicos de la presente guía.
[16] Puede consultar la recomendación general en las Recomendaciones en materia de seguridad de datos personales del INAI en: www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013.

Recursos

Para más información para implementar un sistema de gestión de seguridad de datos o un plan para el manejo de incidentes de seguridad, puede consultar las siguientes herramientas del INAI:

- *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales* puede consultarla en: http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf.

A fin de determinar las medidas de seguridad y los niveles de acceso a los datos que se deben de implementar, de acuerdo a las recomendaciones del INAI para implementar un Sistema de Gestión de Datos Personales, se debe realizar un inventario de todos los datos personales y sensibles que se recaban para realizar posteriormente un análisis de los siguientes factores: el riesgo inherente a los tipos de datos personales que se tratan y su sensibilidad, el desarrollo tecnológico, las posibles consecuencias de la vulneración de la seguridad de los datos para los titulares, el número de titulares de los que se colectan datos, las vulnerabilidades a la seguridad previas ocurridas, el riesgo por el valor potencial de los datos personales tratados por un tercero no autorizado y demás factores que puedan incidir en los niveles de riesgos y afectación a las personas migrantes. Para facilitar la elaboración del inventario y este análisis se sugiere retomar el diagnóstico y mapeo de datos del Anexo 1 de la presente guía.

Para medir la sensibilidad de los datos personales es importante reflexionar sobre las posibles consecuencias que habría si esos datos estuvieran a disposición de personas no autorizadas y verificar:

a) **Si es posible que derive en actos discriminatorios hacia el titular.** Por ejemplo, si se filtra la información de la orientación sexual de una beneficiaria quien solicitó que este dato permaneciera confidencial ya que ha tenido experiencias discriminatorias en otros albergues.
b) **Si puede causar daños al interesado.** Por ejemplo, si la fotografía de un migrante que fue víctima del delito circulara en redes sociales y como posible consecuencia ponga en alerta a los agresores de su ubicación implicando un riesgo a la integridad de la persona.
c) **Si puede causar daños a otros interesados.** Por ejemplo, si por un incidente de seguridad se filtran los datos de contacto de emergencia de los beneficiarios con personas del crimen organizado y como posible consecuencia haya llamadas de extorsión con sus familiares.

d) **Si puede causar daños al personal del albergue y a terceros autorizados.** Por ejemplo, en caso de que se filtre la denuncia realizada por una persona migrante y como consecuencia se intimide al personal jurídico del albergue que le ha proporcionado apoyo en la materia.

Recursos

Para más información para sobre cómo realizar el análisis de riesgo puede consultar la siguiente herramienta del INAI:

- *Metodología de Análisis de Riesgo BAA* disponible en: http://inicio.inai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf.

A su vez, el albergue deberá evaluar las medidas de seguridad con las que ya cuenta tomando en consideración la cultura del personal, el entorno de trabajo físico y el entorno de trabajo digital para detectar cuáles prácticas han sido efectivas para la protección de datos y cuáles son inadecuadas en cada uno de estos rubros, de manera que podrían vulnerar la seguridad de los datos. A continuación, se plantean algunos ejemplos de prácticas inadecuadas:

a) **Culturales:** no contar con políticas de respaldo periódico de datos, dejar expedientes de beneficiarios al alcance de cualquiera, tener anotadas las contraseñas de los correos en un papel a la vista de cualquier persona, no contar con políticas de eliminación y borrado de datos personales, no contar con bitácoras que registren las salidas y entradas de quienes acceden al albergue.
b) **Entorno físico:** no contar con archiveros con llaves o cerraduras en las puertas de los espacios donde se guardan los datos personales y sensibles, trabajar con los documentos originales cuando se sale del albergue (se pueden perder o dañar en el movimiento), guardar los documentos en un espacio con humedad, etc.
c) **Entorno digital:** no actualizar *software*, no usar *antimalware*, no respaldar la información, no cambiar las contraseñas de manera periódica para acceder a los equipos/correos.

A partir de esta revisión se puede hacer un análisis de brechas, de manera que se comparen las prácticas existentes contra las que se debería de tener.

Recursos

El INAI cuenta con una herramienta que permite registrar y documentar las medidas existentes y faltantes del albergue de manera que pueda evaluar sus vulneraciones.

- *Evaluador de Vulneraciones* disponible en:
  http://inicio.ifai.org.mx/SitePages/Evaluador-Vulneraciones.aspx.

A partir del análisis de riesgos, donde se detecten las amenazas y vulnerabilidades a la seguridad de los datos personales, las posibles afectaciones que habría en caso de que ocurrieran o se cumplieran estas amenazas o vulneraciones y las probabilidades de que se materialicen las amenazas, el albergue diseñará un plan de trabajo que establezca de manera clara y precisa, las medidas de seguridad que se implementarán, las personas que deberán cumplir con las medidas, el periodo de duración de las acciones y los recursos que se destinarán para el cumplimiento del plan.

Algunas medidas de seguridad que pueden ayudar a proteger los datos son:

Medidas de seguridad

Administrativas

- Capacitar al personal sobre protección de datos y seguridad.
- Establecer reglamentos sobre el acceso y uso de información sensible, restringiendo acceso a personal y terceros.
- Fomentar la cultura de la seguridad de la información.
- Políticas de consentimiento y limitación de toma y uso de fotografías.

Técnicas

- Manejo obligatorio de contraseñas seguras para acceder a equipos de cómputo, teléfonos smartphone y correo del personal del albergue.
- Uso de correos institucionales o contar con correos de uso exclusivo del albergue.
- Proteger los equipos de cómputo y/o teléfonos inteligentes con software antivirus y cortafuegos.
- No conectarse a redes no confiables.
- Borrado seguro de datos.
- Calendarizar respaldo de información.
- Usar el bloqueo automático de pantallas.
- No manejar datos sensibles en dispositivos portátiles como teléfonos, tabletas, USB.
- No compartir datos en redes sociales: WhatsApp, Facebook, etc.
- Cambiar las contraseñas de acceso periódicamente.
- Actualizar contraseñas según cambie el usuario.
- Uso de mecanismos de cifrado de la información para compartir datos sensibles.

Físicas

- Guardar la información en espacios privados.
- Uso de archiveros con llaves.
- Destrucción segura de documentos.
- Manejo de cámaras, equipos de seguridad, cerraduras, candados.
- Aprobación de salida de documentos, equipo o medios de almacenamiento.
- Política escritorio limpio.
- Clasificar los registros de datos por grado de sensibilidad de la información.
- Restringir accesos a personal o voluntarios a los espacios o equipos de cómputo en donde haya tratamiento de datos personales/sensibles.

Se deberá compartir el plan y capacitar al personal que realice **tratamiento de datos personales** para que las medidas y políticas de seguridad sean implementadas. El plan deberá ser monitoreado, evaluado y actualizado de manera periódica.

Finalmente, es primordial contar con un plan de respuesta para incidentes de seguridad, el cual debe incluir el proceso de notificación de vulneración a la seguridad de los **datos personales** al **titular**. La notificación deberá informar a los titulares del derecho la naturaleza del incidente, los **datos personales** comprometidos, recomendaciones sobre medidas que se pueden adoptar para proteger los intereses del **titular**, las acciones correctivas que se han realizado y los medios donde puede **obtener más información al respecto**.

Recursos

Para más información sobre cómo elaborar un plan de seguridad de datos personales o de manejo de incidentes puede consultar las siguientes herramientas del INAI:

- Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas disponible en: http://inicio.inai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mpymes (Julio2015).pdf.

- Recomendaciones para el manejo de incidentes de seguridad de datos personales puede consultarlas en: http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf.

Anexos

ANEXO 1. Mapeo de datos personales y diagnóstico de protección de datos personales

Manejo de datos	Sí	¿Quién(es) los manejan?	No
¿La organización recaba datos personales?			
¿La organización usa datos personales?			
¿La organización almacena datos personales?			
¿La organización borra datos personales?			
¿La organización recaba datos sensibles?			
¿La organización usa datos sensibles?			
¿La organización usa datos sensibles?			
¿La organización almacena datos sensibles?			

Tipos de Datos personales/sensibles	¿Ya se recaba? Sí	No	Necesario Sí	No	Tipo de sensibilidad o nivel de riesgo inherente
Nombre					
Edad					
Sexo					
Correo					
Teléfono					
Estado civil					
Domicilio					
Firma					
Datos personales sensibles	**Sí**	**No**	**Sí**	**No**	**Tipo de sensibilidad o nivel de riesgo inherente**
Religión					
Estado de salud					
Orientación sexual					
Identidad de género					
Pertenencia a grupo étnico					
Estatus migratorio					
Víctima de delito					
Antecedentes penales					
Situación jurídica					
Razones de proyecto migratorio					

Formato de obtención de datos personales	Físico	Digital	Personas/áreas con acceso
(Ejemplos) Entrevista de personas			
Correos electrónicos			
Listas de registro entradas/salidas albergue			
Bases de datos			
Pertenencia a grupo étnico			
Copias de documentos de identidad (pasaporte, CURP, etc.)			
Expedientes			

Tabla mapeo almacenamiento y transferencia de datos

¿De quién se obtiene los datos personales?	¿Qué área maneja sus datos?	¿Cuál es el motivo del manejo de sus datos?	¿Por cuánto tiempo almacenan los datos?	¿Se comparten estos datos con externos al albergue?	¿Con quiénes se comparten y por qué?
(Ejemplos) Personas migrantes					
Asistentes talleres					
Voluntarios					
Personal					
Trabajadores sociales					

Tipo de documento con datos personales	Sitio de resguardo	¿Quién tiene acceso al sitio?
(Ejemplos) Correos: atencion@albergue.com; contacto@albergue.com	*(Ejemplos) Computadora de escritorio asistencia*	
Correo; juridico@albergue.com; carpeta jurídico: expedientes de casos Archivo: canalización.xls	*Computadora portátil jurídico*	
Expedientes de casos	*Archivero jurídico*	
Entrevista de personas	*Cajón escritorio*	
Correos electrónicos de jurídico, fotos de expediente	*Smartphone Abogado*	
Respaldo de base de datos de canalización	*Memoria USB*	
Fotos de personas migrantes	*CD*	
Respaldos de listas de registro de entradas	*Dropbox/ Google Drive*	

Diagnóstico de protección de datos personales

Protección de datos	Sí	No
¿Se cuenta con Aviso de Privacidad?		
¿Se cuenta con un formato de consentimiento informado para tomar fotografías?		
¿El personal/voluntarios firman una Carta compromiso de confidencialidad?		
¿Se cuenta con medidas de seguridad para proteger los datos personales?		

Calidad	Sí	No
¿Se ha explicado al personal y/o voluntarios la importancia de contar con datos veraces y cuáles son las posibles consecuencias de trabajar con datos inexactos?		
¿Los espacios en los que se obtienen los datos garantizan un entorno seguro para que las personas provean sus datos personales y/o sensibles?		
¿Los espacios en los que se obtienen los datos garantizan un entorno seguro para que las personas provean sus datos personales y/o sensibles?		
¿Se ha promovido con el personal y/o los voluntarios del albergue la importancia de la confidencialidad de los datos?		
¿Se cuenta con prácticas para que las personas migrantes validen que sus datos proporcionados son correctos?		
¿Los documentos y registros electrónicos se almacenan en medios seguros que están protegidos de riesgos de seguridad y acceso no autorizado?		
¿Los documentos y registros en papel se almacenen en lugares seguros que previenen el desgaste y el acceso no autorizado?		
¿Se realiza respaldo de la información regularmente?		
Tanto los documentos físicos y electrónicos son legibles y están actualizados.		

Relevancia	Sí	No
¿Se ha visto afectada la calidad de los datos por alguna inexactitud?		
¿Hubo algún cambio en los procesos del albergue que hizo que el registro de algunos datos personales sea innecesario?		
¿Hasta qué punto los datos personales recabados siguen cumpliendo su función, es necesario mantener su almacenamiento?		
En cuanto a los datos personales que han cumplido con su finalidad y ya no es necesario almacenar ¿han pasado por un proceso de eliminación o borrado?		
Sobre los datos personales que ya cumplieron su finalidad ¿pueden servir para propósitos estadísticos o de investigación que sean compatibles con las finalidades para las cuales fueron originalmente pensados?		

Diagnóstico de protección de datos personales

Seguridad de los datos	Sí	No
¿Los datos personales están clasificados de acuerdo con el tipo de sensibilidad o nivel de riesgo inherente?		
¿Existe un análisis del nivel de seguridad para cada área de trabajo según el acceso, uso y transferencia de datos personales y conforme al grado de sensibilidad y confidencialidad de los datos que manejan?		
¿Se ha identificado algún factor ambiental, técnico o humano que vulnere la seguridad de los datos?		
¿Se cuenta con planes para el caso que se pierda la información?		
¿Se ha evaluado si los espacios y equipos de almacenamiento de datos personales son seguros?		
¿Existen debilidades en los sistemas de almacenamiento o en los sistemas de cómputo?		
¿Se cuenta con un plan para reducir los riesgos tomando en cuenta las medidas de seguridad operativas, técnicas y físicas existentes?		

ANEXO 2. Ejemplos de Avisos de Privacidad Modelo para Albergues

a) Ejemplo de Aviso de privacidad integral

Aviso de privacidad para personas usuarias o posibles usuarias de los servicios de Albergue Camino Amigo

Identidad y domicilio del responsable de la protección de datos personales

Con fundamento en la Ley Federal de Protección de Datos Personales en Posesión de Particulares publicada el 5 de julio de 2010 en el Diario Oficial de la Federación, el Albergue Camino Amigo con domicilio en Avenida Venustiano Carranza 1199, Col. Del Valle, San Luis Potosí, SLP, C.P. 78200 es el/la responsable del uso y protección de sus datos personales/datos personales sensibles y al respecto le informa lo siguiente:

Finalidades y uso de los datos

Los datos personales que recabamos se utilizarán para las siguientes finalidades que son necesarias para otorgar nuestros servicios:

- Para el registro de entrada y salida de las instalaciones.
- Para su identificación, localización y contacto.
- Para la integración de su expediente, brindar información y orientación.
- Para brindar asistencia médica y psicológica.
- Para la evaluación y la canalización de casos que requieran de asistencia y apoyo de emergencia de instituciones especializadas.

De manera adicional, utilizaremos su información personal para las siguientes finalidades que no son necesarias para el servicio solicitado, pero que nos permiten y facilitan brindarle una mejor atención:

- Difusión en medios de comunicación o redes sociales sobre las problemáticas que enfrentan las personas usuarias de los servicios del Albergue Camino Amigo.
- Avisar a sus familiares o consulado en caso de algún accidente o que no sea posible localizarle.

En caso de que no desee que sus datos personales sean tratados para estos fines adicionales, desde este momento usted nos puede comunicar lo anterior, marcando los recuadros que se presentan a continuación:

No consiento que mis datos personales sean usados para las siguientes finalidades:

- ☐ Difusión en medios de comunicación o redes sociales sobre las problemáticas que enfrentan las personas usuarias de los servicios del Albergue Camino Amigo.
- ☐ Avisar a sus familiares o consulado en caso de algún accidente o que no sea posible localizarle.

En caso de no aceptar el uso de sus datos personales para estas finalidades, no podrá ser un motivo para que le neguemos los servicios y productos que solicita o contrata con nosotros. Si usted no manifiesta su negativa para las finalidades secundarias antes mencionadas, entendemos que nos otorga su consentimiento para tratar sus datos personales en ese sentido.

Obtención de datos

a) Datos personales

Para las finalidades antes señaladas el Albergue Camino Amigo podrá recabar los siguientes datos personales:

- Datos de identificación (nombre completo; estado civil; firma autógrafa lugar y fecha de nacimiento; nacionalidad; fotografía; edad).
- Datos de contacto (correo electrónico; teléfono celular).
- Datos de contacto en caso de emergencia (nombre completo, teléfono fijo y celular, correo electrónico).
- Datos sobre su idioma.
- Datos sobre su condición migratoria.
- Datos sobre el tipo de atención y trámite que solicita al Albergue Camino Amigo.

b) Datos personales sensibles

Además de los datos personales mencionados anteriormente para las finalidades informadas, en el presente aviso de privacidad utilizaremos los siguientes datos personales considerados como sensibles, que requieren de especial protección:

- Datos sobre si forma parte o no de la comunidad LGBT.
- Datos sobre estado de salud física y/o mental.
- Datos de origen étnico o racial.
- Datos sobre su contexto familiar.
- Datos sobre si ha sido víctima de algún delito.
- Datos sobre antecedentes penales.
- Datos sobre creencias religiosas, posturas ideológicas y opiniones políticas.
- Datos sobre motivos de salida de país de origen.
- Datos sobre sus intenciones o proyecto migratorio.

c) Datos personales de menores de edad (sólo si aplica)

Entendemos que usted cuenta con las facultades para actuar en calidad de padre o tutor o como quien ejerce la patria potestad y representación legal del menor de edad de conformidad con las reglas de representación dispuestas en el Código Civil Federal.

Si usted no desea que los datos personales del menor de edad sean utilizados para las finalidades señaladas en el presente aviso de privacidad, usted nos puede comunicar lo anterior, marcando una X en el recuadro siguiente:

☐ No autorizo el tratamiento de datos personales del menor de edad.

Transferencia de datos personales y para qué fines

Destinatario de los datos personales	Finalidad
Autoridades migratorias y administrativas mexicanas y/o extranjeras.	Para llevar a cabo los trámites migratorios y administrativos necesarios para regularizar su situación jurídica y llevar a cabo las acciones necesarias para la defensa de sus derechos*.
Instituciones donantes.	Para reportar los avances y resultados de los proyectos en los que intervienen y cumplir con los compromisos que se establecen en los convenios de colaboración con estas instituciones.
Instituciones de salud del sector público y privado.	Para brindar asistencia médica a las personas que lo requieran. NOTA: la información de su estado de salud será manejada con completa confidencialidad. En los casos que se encuentre en riesgo su vida o su integridad no se requerirá de su consentimiento.

Le informamos que para las transferencias indicadas con un asterisco (*) requerimos obtener su consentimiento.

En caso de que no desee que sus datos personales sean transferidos a estas instituciones desde este momento usted nos puede comunicar lo anterior, marcando el recuadro que se presenta a continuación:

No autorizo que mis datos personales sean compartidos con los siguientes terceros:

☐ Autoridades migratorias y administrativas mexicanas y/o extranjeras.
☐ Instituciones de salud del sector público y privado.

Si usted no manifiesta su negativa para dichas transferencias, entenderemos que nos ha otorgado el consentimiento.

Mecanismo para Acceder, Rectificar o Cancelar sus datos personales, u Oponerse a su uso (ejercicio de derechos ARCO)

Como titular de sus datos personales, usted tiene derecho a conocer qué datos personales tenemos, para qué los utilizamos y las condiciones del uso que les damos (Acceso). Asimismo, es su derecho solicitar que se corrija su información en caso de que esté desactualizada, sea inexacta o incompleta (Rectificación); instruir que se elimine de nuestros registros o bases de datos cuando considere que los datos no están siendo utilizados conforme a los principios, deberes y obligaciones previstas en la normativa aplicable (Cancelación); o bien oponerse al uso de sus datos personales para fines específicos (Oposición). Estos derechos se conocen como derechos ARCO.

Para ejercer cualquiera de sus derechos ARCO y conocer más sobre el proceso, usted puede presentar su solicitud en el correo protecciondedatos@alca.org.mx o solicitar el apoyo en el llenado de la solicitud con nuestro departamento de Protección de Datos ubicado en Avenida Venustiano Carranza 1199, Col. Del Valle, San Luis Potosí, SLP, C.P. 78200 o en el teléfono 444.123.5678 donde se atenderá cualquier duda que pudiera tener sobre el tratamiento de su información y dará trámite a las solicitudes para el ejercicio de sus derechos ARCO.

Mecanismo de revocación del consentimiento para el uso de datos personales

Usted puede revocar el consentimiento que, en su caso, nos haya otorgado para el tratamiento de sus datos personales. Sin embargo, es importante que tenga en cuenta que no en todos los casos podremos atender su solicitud o concluir el uso de forma inmediata, ya que es posible que por alguna obligación legal requiramos seguir tratando sus datos personales. Asimismo, usted deberá considerar que para ciertos fines, la revocación de su consentimiento implicará que no le podamos seguir prestando el servicio que nos solicitó, o la conclusión de su relación con nosotros.

Para revocar su consentimiento deberá presentar su solicitud escrita o solicitar el apoyo en el llenado de la solicitud en el departamento de Protección de Datos o enviar un correo electrónico a protecciondedatos@alca.org.mx.

Para conocer el procedimiento y requisitos para la revocación del consentimiento, usted podrá llamar al tel. 444.123.5678 o bien ponerse en contacto con nuestro departamento de Protección de Datos.

Medios para limitar el uso o divulgación de sus datos personales

Para limitar el uso o divulgación de sus datos personales, ponemos a su disposición la dirección de correo electrónico protecciondedatos@alca.org.mx a efecto de ser inscrito en nuestro listado de exclusión interno denominado "Titulares sin autorización para el tratamiento de sus datos personales para fines secundarios", a fin de que sus datos personales no sean tratados para las finalidades secundarias previstas en este documento.

Uso de *cookies*, *web beacons* u otras tecnologías similares No se hace uso *cookies*, *web beacons* u otras tecnologías que permitan recabar sus datos personales de manera automática y simultánea.

Cambios en el aviso de privacidad

El presente aviso de privacidad puede sufrir modificaciones, cambios o actualizaciones derivadas de nuevos requerimientos legales; de nuestras propias necesidades por los productos o servicios que ofrecemos; de nuestras prácticas de privacidad; o por otras causas.

Nos comprometemos a mantenerle informado sobre los cambios que pueda sufrir el presente aviso de privacidad, a través de nuestra página de internet www.alberguecaminoamigo.org.

El procedimiento a través del cual se llevarán a cabo las notificaciones sobre cambios o actualizaciones al presente aviso de privacidad es el siguiente: publicación en nuestra página de internet y a través de correo electrónico con nuestra base de contactos.

Consiento que mis datos personales y sensibles sean tratados conforme a los términos y condiciones del presente Aviso de Privacidad

_____

Nombre del titular

_____

Firma del titular

_____

Lugar y fecha

Última actualización [13/02/2019].

b) Ejemplo de Aviso de privacidad simplificado

Aviso de privacidad para personas usuarias o posibles usuarias de los servicios de Albergue Camino Amigo

Identidad y domicilio del responsable de la protección de datos personales

Con fundamento en la Ley Federal de Protección de Datos Personales en Posesión de Particulares publicada el 5 de julio de 2010 en el Diario Oficial de la Federación, el Albergue Camino Amigo con domicilio en Avenida Venustiano Carranza 1199, Col. Del Valle, San Luis Potosí, SLP, C.P. 78200es el/la responsable del uso y protección de sus datos personales/ datos personales sensibles y al respecto le informa lo siguiente:

Finalidades y uso de los datos

Los datos personales que recabamos se utilizarán para las siguientes finalidades que son necesarias para otorgar nuestros servicios:

- Para el registro de entrada y salida de las instalaciones.
- Para su identificación, localización y contacto.
- Para la integración de su expediente, brindar información y orientación.
- Para brindar asistencia médica y psicológica.
- Para la evaluación y la canalización de casos que requieran de asistencia y apoyo de emergencia de instituciones especializadas.

De manera adicional, utilizaremos su información personal para las siguientes finalidades que no son necesarias para el servicio solicitado, pero que nos permiten y facilitan brindarle una mejor atención:

- Difusión en medios de comunicación o redes sociales sobre las problemáticas que enfrentan las personas usuarias de los servicios del Albergue Camino Amigo.
- Avisar a sus familiares o consulado en caso de algún accidente o que no sea posible localizarle.

En caso de que no desee que sus datos personales sean tratados para estos fines adicionales, desde este momento nos lo puede comunicar contactando al departamento de Protección de Datos Personales en el correo protecciondedatos@alca.org.mx o en el teléfono 444.123.5678 o en las oficinas ubicadas en Avenida Venustiano Carranza 1199, Col. Del Valle, San Luis Potosí, SLP, C.P. 78200.
En caso de no aceptar el uso de sus datos personales para estas finalidades, **no podrá ser un motivo** para que le neguemos los servicios y productos que solicita o contrata con nosotros.

Para conocer mayor información sobre los términos y condiciones en que serán tratados sus datos personales, como los terceros con quienes compartimos su información personal y la forma en que podrá ejercer sus derechos ARCO, puede consultar el aviso de privacidad integral en nuestra página de internet www.alberguecaminoamigo.org.

c) Ejemplo de Aviso de privacidad corto

El Albergue Camino Amigo con domicilio en Avenida Venustiano Carranza 1199, Col. Del Valle, San Luis Potosí, SLP, C.P. 78200 utilizará sus datos personales y sensibles para las siguientes finalidades: el registro de entrada y salida de las instalaciones; su identificación, localización y contacto; la integración de su expediente, brindar información y orientación; brindar asistencia médica y psicológica y la evaluación, la canalización de casos que requieran de asistencia y apoyo de emergencia de instituciones especializadas, la difusión en medios de comunicación o redes sociales sobre las problemáticas que enfrentan las personas usuarias de los servicios del Albergue Camino Amigo y avisar a sus familiares o consulado en caso de algún accidente o que no sea posible localizarle. Para más información acerca del tratamiento y de los derechos que puede hacer valer, usted puede acceder al aviso de privacidad integral a través de nuestra página de internet www.alberguecaminoamigo.org.

ANEXO 3. Formato de Consentimiento para tomar grabaciones de imagen, video o audio de las personas migrantes

(Nombre del albergue o nombre de la organización que visita el albergue)
Consentimiento para tomar grabaciones de imagen, video o audio de las personas migrantes

El albergue/organización_____ es responsable del uso y protección de los datos personales que usted autorice compartir. Los datos personales que recabamos son:

a) Imágenes
b) Video
c) Voz

El albergue/organización_____ se compromete a no grabar imagen, audio o video de usted sin su consentimiento, a permitirle ver la copia de las grabaciones que fueron tomadas con su consentimiento y a borrar las grabaciones que nos solicite de los medios y redes sociales que se encuentren bajo nuestro control.
Por medio de la presente, yo (nombre de la persona migrante), declaro que:

1) Autorizo al albergue/organización_____ para que el (nombre de quien hará las grabaciones) me tome las grabaciones consentidas.
2) Consiento que se incluya lo siguiente en las grabaciones:
   - ☐ Mi voz
   - ☐ Imagen de mi cara
   - ☐ Imagen de mi cuerpo
   - ☐ Mi nombre verdadero
3) Entiendo y estoy de acuerdo que se utilicen las grabaciones para los siguientes fines:
   - ☐ Las presentaciones informativas del (nombre del albergue/organización)
   - ☐ Los reportes financieros y de resultados para las instituciones donantes
   - ☐ Difusión de las actividades de (nombre del albergue/organización) en sus redes sociales y página de web

Se me informará y solicitará mi consentimiento para el uso de las grabaciones para cualquier otro fin, diferente a los anteriormente citados.
Manifiesto que he leído el presente consentimiento y que entiendo las cláusulas arriba señaladas.

Nombre y firma de la persona migrante

ANEXO 4. Formato de Carta compromiso de confidencialidad

Carta compromiso de confidencialidad

LUGAR Y FECHA

A quien corresponda

Por medio de la presente yo (NOMBRE COMPLETO), manifiesto que en mi capacidad como (CARGO DESEMPEÑADO) tendré acceso a datos personales de las personas migrantes beneficiarias de los servicios e instalaciones del (NOMBRE DEL ALBERGUE).

Entiendo la obligación del albergue de tratar los datos personales de forma confidencial y de respetar los derechos a la privacidad y a la protección de datos personales de las personas migrantes.

Declaro que estoy de acuerdo y me comprometo a:

a) Mantener el anonimato y la confidencialidad de los datos personales de las personas migrantes.
b) Tratar los datos exclusivamente para llevar a cabo y cumplir con las actividades y obligaciones del cargo que desempeño en el albergue.
c) No difundir los datos con personas no autorizadas o ajenas al albergue.
d) Notificar a (PERSONA RESPONSABLE DE PROTECCIÓN DE DATOS) de cualquier incumplimiento a la presente carta o incidente que ponga en riesgo la protección de datos personales.

En caso de incumplir con lo estipulado y compartir con terceros no autorizados se podrá terminar mi relación con el albergue o seré acreedor de las sanciones que el (NOMBRE DEL ALBERGUE) considere pertinentes.

Atentamente

FIRMA

Fuentes de Consulta

FUENTES DE CONSULTA

- Diario Oficial de la Federación (2019). Constitución Política de los Estados Unidos Mexicanos. Recuperado en: www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo14166.pdf.
- Diario Oficial de la Federación (2017). Ley General de Protección de Datos Personales en Posesión de Particulares. Recuperado en: www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo83178.pdf.
- Diario Oficial de la Federación (2011). Reglamento de la Ley General de Protección de Datos Personales en Posesión de Particulares. Recuperado en: www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo88475.pdf.
- Diario Oficial de la Federación (2013). Lineamientos del Aviso de Privacidad. Recuperado en: http://dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013.
- Diario Oficial de la Federación (2013). Recomendaciones en Materia de Seguridad de Datos Personales. Recuperado en: www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013.
- *International Committee of the Red Cross. Handbook on Data Protection in Humanitarian Action*. Recuperado en: www.icrc.org/en/data-protection-humanitarian-action-handbook.
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (s.f). El ABC del aviso de privacidad. Recuperado en: http://abcavisosprivacidad.ifai.org.mx/.
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2015). Guía para el Aviso de Privacidad. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2015). Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales. Recuperado en: http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf.
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2015). Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas. Recuperado en: http://inicio.inai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf.

- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2015). Metodología de Análisis de Riesgo BAA. Recuperado en: http://inicio.inai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf.
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2016). Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Recuperado en: http://inicio.inai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf.
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2016). Introducción a la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2016). Recomendaciones para la designación de la persona o departamento de datos personales. Recuperado en: http://inicio.inai.org.mx/DocumentosdeInteres/RecomendacionesDesignar.pdf.
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2018). Marco Normativo de protección de datos personales en posesión de los particulares. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2018). Recomendaciones para el manejo de incidentes de seguridad de datos personales Recuperado en: http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf.
- Organización de los Estados Americanos (2014). Resolución de la Asamblea General 2842 (XLIV-O/14) Acceso a la Información Pública y Protección de Datos Personales. Recuperado en: www.oas.org/es/sla/ddi/docs/AG-RES_2842_XLIV-O-14.pdf.
- Organización Internacional para las Migraciones (2010). *IOM Data Protection Manual*. Recuperado en: http://publications.iom.int/system/files/pdf/iomdataprotection_web.pdf.
- *Front line defenders. Security in a box*. Recuperado en: http://securityinabox.org/es/guide/malware/.
- Suprema Corte de Justicia de la Nación (s.f). Semanario Judicial de la Federación: *Fundamentación y motivación*. Recuperado en: http://sjf.scjn.gob.mx/sjfsist/paginas/DetalleGeneralV2.aspx?id=394216&Clase=DetalleTesisBL.

OIM
ONU MIGRACIÓN