Guía de
PROTECCIÓN DE DATOS PERSONALES
para las personas titulares en situaciones de emergencia

inai

DIRECTORIO

Blanca Lilia Ibarra Cadena
Comisionada Presidenta

Francisco Javier Acuña Llamas
Comisionado

Adrián Alcalá Méndez
Comisionado

Norma Julieta Del Río Venegas
Comisionada

Oscar Mauricio Guerra Ford
Comisionado

Rosendoevgueni Monterrey Chepov
Comisionado

Josefina Román Vergara
Comisionada

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

Av. Insurgentes Sur 3211,
Col. Insurgentes Cuicuilco,
Alcaldía Coyoacán,
C.P. 04530,
Ciudad de México.

Edición, agosto de 2021

ÍNDICE

PRESENTACIÓN

Debido a la ubicación geográfica, el clima, la topografía y las características, así como las actividades volcánicas y sísmicas, México es vulnerable a una variedad de desastres naturales. De acuerdo con datos de la Secretaría de Seguridad y Protección Ciudadana, en el año 2020, se atendieron a más de 2 millones de personas en situaciones de emergencia o desastre.[1]

Bajo este contexto, la presente Guía pretende exponer, en forma práctica, a las personas titulares cómo los responsables han de proteger sus datos personales ante una situación de emergencia ocasionada por desastres naturales, a partir de los principios que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como lo dispuesto en los Lineamientos Generales de Protección de Datos Personales para el Sector Público, a través de un documento que les permita identificar escenarios que requieran de la protección de sus datos personales.

En este sentido, la presente Guía dará a conocer a las personas titulares de los datos personales qué información se deberá recabar, para qué fines, quién hará el tratamiento y, en su caso, cómo se debe hacer la transferencia o transmisión de ésta.

En virtud de lo anterior, con fundamento en lo dispuesto por el artículo 89, fracciones I, XII y XIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, pone a disposición de las personas titulares la presente Guía de Protección de Datos Personales para las personas Titulares en situaciones de emergencia.

1 Información obtenida de: https://www.gob.mx/sspc/prensa/el-2020-ano-atipico-por-afectaciones-de-fenomenos-naturales-cnpc?idiom=es

GLOSARIO

A efecto de facilitar la comprensión de las presentes recomendaciones, se entenderá por:

Datos personales	Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.[2]
Datos personales sensibles	Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.[3]
INAI o Instituto	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
LGPDPPSO o Ley General	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Organismos garantes	Aquellos con autonomía constitucional especializados en materia de acceso a la información y protección de datos personales, en términos de los artículos 6º y 116, fracción VIII de la Constitución Política de los Estados Unidos Mexicanos.[4]
Responsable(s)	Son los sujetos obligados, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, organismos constitucionales autónomos, tribunales administrativos, partidos políticos, fideicomisos y fondos públicos, que deciden sobre el tratamiento de datos personales.[5]

2 Artículo 3, fracción IX de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

3 Artículo 3, fracción XI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

4 Artículo 3, fracción XXIV de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

5 Artículo 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Situación de emergencia	Situación fuera de lo común que pueda causar un daño a la sociedad y propiciar un riesgo excesivo para la seguridad e integridad de la población en general, generada o asociada con la inminencia, alta probabilidad o presencia de un agente perturbador.[6]
Titular	La persona física identificada e identificable a quien corresponden los datos personales.[7]
Tratamiento	Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.[8]

6 Artículo 2, fracción XVII de la Ley General de Protección Civil.

7 Artículo 3, fracción XXXI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

8 Artículo 3, fracción XXXIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

OBJETIVO

La presente Guía tiene por objeto brindar a las personas titulares herramientas prácticas para promover el cuidado de sus datos personales, al momento de proporcionarlos a los distintos responsables, cuando surjan situaciones de emergencia derivadas de casos fortuitos o de fuerza mayor.

SITUACIONES DE EMERGENCIA ¿CUÁNDO ESTAMOS FRENTE A ELLAS?

Estamos frente a una emergencia, cuando una situación fuera de lo común pueda causar un daño a la sociedad y propiciar un riesgo excesivo para la seguridad e integridad de la población en general, generada o asociada con la inminencia, alta probabilidad o presencia de un agente perturbador;[9] en este caso, los responsables para el tratamiento de los datos personales deberán tomar medidas atendiendo el tipo de emergencia, y seleccionar qué tipo de información requiere para determinar qué datos relevantes son necesarios para atender la situación de emergencia.

Los sujetos obligados competentes en una emergencia deberán para la selección de la información, basarse en objetivos de eficacia y eficiencia, tomando en cuenta los recursos disponibles.

EL CASO FORTUITO Y LA FUERZA MAYOR

La Suprema Corte de Justicia de la Nación ha sostenido como caso fortuito un acontecimiento natural inevitable, previsible o imprevisible, que impida, en forma absoluta, el cumplimiento de una obligación legalmente adquirida. La fuerza mayor, a diferencia del caso fortuito, no es ajena a la voluntad del hombre, pues, depende de la de un tercero distinto de los sujetos de la relación jurídica que impide, en forma absoluta, en cumplimiento de una obligación. A mayor consideración, la fuerza mayor exige, como el caso fortuito, que el hecho impida, de una manera absoluta, el cumplimiento de la obligación.[10]

Las características del caso fortuito o fuerza mayor según la doctrina son los siguientes:

- **Según el evento**. La fuerza mayor se debería a un hecho de la naturaleza, mientras que en el caso fortuito se trataría de un hecho humano.[11]

- **Imprevisibilidad o inevitabilidad**. El caso fortuito es un evento imprevisible aun utilizado una conducta diligente. La fuerza mayor es un evento que, aunque pudiera preverse es inevitable.[12]

9 Artículo 2, fracción XVII de la Ley General de Protección Civil.

10 Séptima Época, Sala Auxiliar, tesis aislada, Semanario Judicial de la Federación, volumen 28, séptima parte, página 17, de rubro: **"CASO FORTUITO Y FUERZA MAYOR. LAS DIFICULTADES DE ORDEN TÉCNICO Y LA INCOSTEABILIDAD DE LA OPERACIÓN NO CONSTITUYEN CASO FORTUITO NI FUERZA MAYOR Y, POR LO TANTO, SI EL ACTOR, ESTIMANDO LO CONTRARIO, DEMANDÓ LA RESCISIÓN DEL CONTRATO RESPECTIVO, LA ACCIÓN EJERCITADA RESULTA IMPROCEDENTE"**.

11 Revista de Ciencias Jurídicas No. 123 (69-98) septiembre-diciembre 2010. CASO FORTUITO Y FUERZA MAYOR DIFERENCIA COCEPTUAL. Ms C. Jorge Jiménez Bolaños.

12 ÍDEM

Cuando exista una situación provocada por un caso fortuito o de fuerza mayor, conforme a las características citadas anteriormente, el sector público dependiendo de la emergencia emitirá la declaratoria o medidas correspondientes.

En atención a ello, los sujetos obligados podrán adoptar medidas para proteger los datos personales ante este tipo de situaciones, mediante una planificación que le permita identificar y categorizar la información necesaria que va a solicitar a las personas titulares en cada situación de emergencia.

Los Casos Fortuitos o Fuerza Mayor incluirán en forma enunciativa, más no limitativa, los siguientes hechos o actos:

- ***fenómenos de la naturaleza tales como*** tormentas, huracanes, inundaciones, deslaves, relámpagos y terremotos; incendios, pandemias, epidemias, etc.

- ***acontecimientos provocados por el hombre tales como*** actos de guerra (declarada o no); disturbios civiles, motines, insurrecciones, sabotajes y terrorismo; desastres por traslado de Materiales peligrosos, huelgas, cuarentenas, etc.

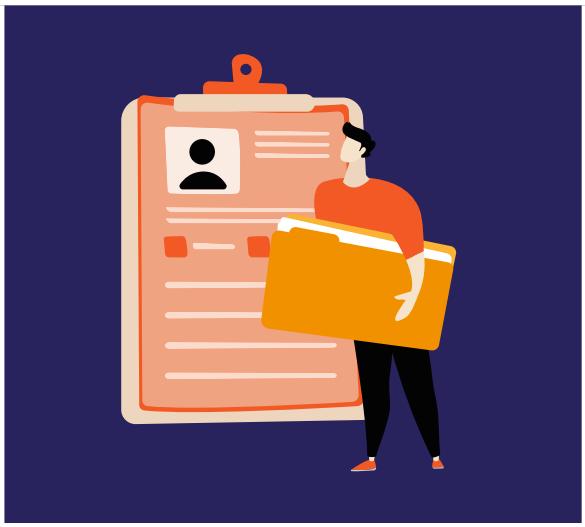
Es por ello por lo que recomendamos a las personas titulares de los datos personales identifiquen qué categoría de datos personales le podrán ser solicitados en una situación de emergencia. Para tal efecto a continuación se señalan las categorías de los datos personales.

CATEGORÍAS DE DATOS PERSONALES RELEVANTES Y ADECUADAS EN UNA SITUACIÓN DE EMERGENCIA

En caso de que se presente una situación de emergencia, los responsables a fin de evitar solicitar datos irrelevantes que no atiendan a las necesidades propias de la emergencia, podrá recabar los datos personales necesarios, sin dejar de observar los principios que señala la Ley General y los Lineamientos Generales.

Para ello, es importante identificar y categorizar cuáles serían los datos relevantes y adecuados a cada situación de emergencia. A continuación, mostramos de manera enunciativa más no limitativa las categorías de datos personales que el responsable podrá considerar:

CATEGORÍAS DE DATOS PERSONALES:



Identificación

Nombre, edad, domicilio, teléfono, correo electrónico, fecha de nacimiento, nacionalidad, estado civil, sexo, RFC, CURP...

Patrimoniales

Cuentas bancarias, saldos, propiedades. Información fiscal, historial crediticio, ingresos y egresos, bienes inmuebles, socioeconómicos.

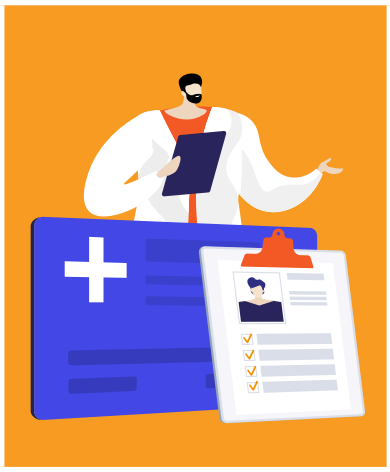
Académicos

Trayectoria educativa, título, número de cédula profesional, certificados y acreditaciones.

Procedimientos Judiciales

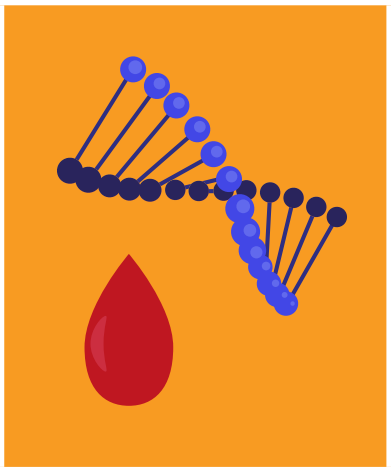
Datos de expedientes judiciales o de procedimientos seguidos en forma de juicio, resoluciones, etc.

CATEGORÍAS DE DATOS PERSONALES SENSIBLES:



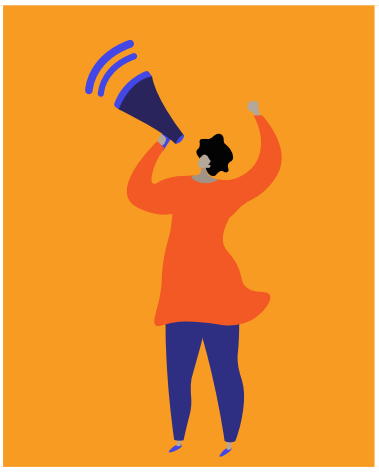
Salud

El estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico.



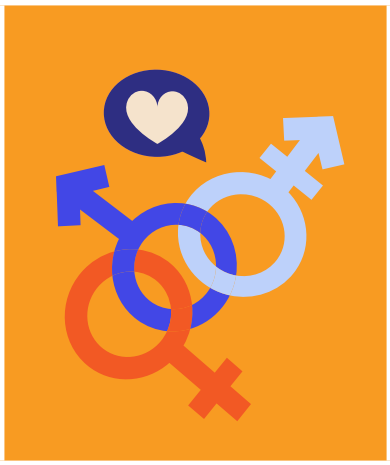
Características biológicas

Tipo de sangre, ADN,...



Ideológicos

Creencias religiosas, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas.



Habitos de Vida y hábitos sexuales

Preferencias u orientación sexual.

Características Físicas

Estatura, peso, color de piel, iris y cabello, señales particulares, etc.

Orígen etnico y racial

Si pertenece a alguna etnia o grupo racial.

Las decisiones que se tomen con respecto a los datos que se recabarán en una situación de emergencia por caso fortuito o de fuerza mayor, deberá de tomarlas el responsable que sea competente de ejecutarlas, las cuales se sugiere se ejecuten de manera oportuna y vayan acorde con los planes de emergencia y los programas de gestión del riesgo que emitan las autoridades al respecto.

Importante:

En una situación de emergencia los datos que se recaben deben guardar coherencia con los planes de emergencia y los programas de gestión del riesgo que emitan las autoridades

Los responsables deben ser comprometidos, sobre las medidas que adopten en respuesta a una situación de emergencia, garantizando a la persona titular que los datos que se recaban serán utilizados para los fines que le ha informado.

Adicional a lo previamente señalado, ante alguna situación de emergencia derivada de caso fortuito o fuerza mayor como un terremoto, pandemia, inundación; etc., se ha detectado que pueden llegar a presentarse riesgos en el tratamiento de datos personales.

Ante ello, se sugiere a las personas titulares de los datos personales estén alertas sobre posibles abusos que pudieran sufrir a través de los diversos medios cuando ocurre una situación de emergencia en los que se puede llegar a difundir información falsa, mensajes informativos con enlaces maliciosos, robo de datos personales a través de falsos beneficios o apoyos, promesas de trabajo, supuestas invitaciones a servicios gratuitos, mensajes ***smishing*** es una palabra compuesta por "SMS" (servicios de mensajes cortos, más conocidos como mensajes de texto)[13] estos mensajes que afirman ser de tu banco y te pide información personal o financiera, como tu número de cuenta o de tu tarjeta bancaria, a través de supuestos mensajes de retiros indebidos, mensajes ***phishing*** (cuando los cibercriminales envían correos electrónicos fraudulentos que intentan engañar al destinatario para que abra un archivo adjunto cargado de malware o haga clic en un enlace malicioso)[14].a través de estos correos electrónicos se solicita al cliente sus datos de cuenta y clave de acceso, simulando una página legítima de un establecimiento incluso una institución de gobierno.

En este sentido, como persona titular de tus datos personales debes tener cuidado a quien se los proporcionas, toda vez que cuando los sujetos obligados requieran algunos de estos, es su deber garantizarte que en el tratamiento se protegerá la confidencialidad sobre cualquier dato personal o personal sensible relacionado con cualquier situación de emergencia. Asimismo, cerciórate que la autoridad que lo solicite sea la competente para atender el escenario, y sobre todo, para hacer uso de tu información personal.

13 La definición puede ser consultada en el siguiente enlace: https://www.kaspersky.es/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

14 La definición puede ser consultada en el siguiente enlace: https://www.kaspersky.es/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

TRATAMIENTO DE DATOS SENSIBLES

En una situación de emergencia el bien tutelado primordial será la vida y la seguridad de la población; sin embargo, este escenario trae aparejado –igualmente– tutelar el derecho humano a la protección de sus datos personales consagrado en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos; por lo que es de vital importancia, que ante una situación de emergencia se considere también como prioridad la protección de los datos personales a fin de evitar poner aún más en riesgo a la población.

De este modo, es necesario que la protección de datos personales deba garantizarse aún más en cualquier situación de emergencia, por lo que el responsable del tratamiento de los datos personales deberá atender a las disposiciones legales en la materia, así como aquellas medidas que se hayan adoptado de manera extraordinaria para enfrentar la emergencia en particular.

Así, en el caso del tratamiento de **datos personales sensibles** en una emergencia **que no pueda dañar a la persona titular en su integridad y sus bienes,** se debe obtener su **consentimiento expreso y por escrito** para su tratamiento, a través de:

- Firma autógrafa.
- Firma electrónica.
- Huella dactilar.
- Cualquier mecanismo de autenticación que al efecto se establezca.

En el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior de la niña, el niño y el adolescente, en términos de las disposiciones legales aplicables.[15]

Sin demérito de lo anterior, es preciso señalar **que no será necesario que el responsable recabe el consentimiento del titular para realizar el tratamiento de los datos personales,** en los siguientes casos:[16]

- **Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes**.

- Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla.

- Cuando las transferencias que se realicen entre responsables sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.

15 Artículo 7 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

16 Artículo 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

- Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente.
- Para el reconocimiento o defensa de derechos del titular ante autoridad competente.
- Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.
- Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria.
- Cuando los datos personales figuren en fuentes de acceso público.
- Cuando los datos personales se sometan a un procedimiento previo de disociación.
- Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

PRINCIPIOS

Los responsables del tratamiento de datos personales en situaciones de emergencia también deberán atender los datos personales de las personas titulares, bajo los principios de licitud, finalidad, lealtad, consentimiento, proporcionalidad, información y responsabilidad, previstos en los artículos 16 de la Ley General y 7 de los Lineamientos Generales de Protección de Datos Personales del Sector Público, y que a continuación se describen:

LICITUD

Los responsables del tratamiento de los datos personales deben sujetarse a las facultades o atribuciones que la normatividad en la materia le confiera. En ese sentido, el responsable sólo podrá hacer con los datos personales aquello que esté legalmente permitido, como cualquier acto de autoridad.

El principio de licitud significa que el tratamiento de datos personales es una actividad que depende de las atribuciones o facultades que previamente le otorga la ley a los Sujetos Obligados, en consecuencia, no deben tratarse datos personales si no se tienen facultades previamente otorgadas.[17]

Ante una situación de emergencia, las decisiones que se tomen con respecto a los datos que se recabarán, deberá tomarlas el responsable que cuente con las facultades para ejecutarlas, considerando que, en esos contextos, los datos personales deberán ser tratados aquellos que sean estrictamente necesarios.

FINALIDAD

El principio de finalidad tiene como propósito que el tratamiento de los datos personales se utilice para el fin que se ha determinado, relacionándolo con las actividades propias del responsable que está recabando la información.

Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, podrá tratar datos personales por razones distintas a las establecidas en el aviso de privacidad, siempre que obtenga el consentimiento del titular y tenga facultades para ello.

Como se ha dicho en líneas anteriores, en el aviso de privacidad se dará a conocer al titular la o las finalidades para las cuales serán tratados los datos personales. ***En el caso que los datos personales y personales sensibles se utilicen para una determinada situación de emergencia, se deberá incluir en el aviso de privacidad esta situación como una finalidad más.***

17 Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados. Disponible en el siguiente enlace: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/_GuiaPrincipiosDeberes.pdf

Los datos personales y personales sensibles que se recaben no deberán ser utilizados para finalidades distintas, que no resulten compatibles o análogas a aquéllas para las cuales fueron recabados, y deberán estar debidamente justificadas, fundamentadas y motivadas, en caso fortuito o de fuerza mayor.

LEALTAD

En cumplimiento a este principio, el responsable deberá apegarse al cumplimiento de la norma y no debe recabar datos personales por medios engañosos o fraudulentos, desleales que propicien discriminación injusta o arbitraria contra las personas titulares, lo que implica que el responsable:

- No recabe datos personales con dolo, mala fe o negligencia.
- Privilegie los intereses del titular, de tal manera que su tratamiento no genere discriminación o un trato injusto contra las personas titulares.
- No vulnere la confianza del titular con relación a que sus datos personales serán tratados conforme a lo acordado.
- Informe todas las finalidades del tratamiento en el aviso de privacidad.

En caso de situaciones de emergencia, las personas titulares deberán cerciorarse por los medios oficiales de comunicación de los responsables, cuáles son los medios por los cuales se recabarán sus datos, a fin de evitar que de forma fraudulenta, con dolo, mala fe, o por medios engañosos sean recabados los mismos, por lo que el tratamiento de los datos personales por parte del responsable deberá ser leal, honesto, ético ante los derechos de las personas titulares, para generar confianza y tener la convicción de que el responsable actúa de buena fe y en cumplimiento a las normas legales aplicables.

CONSENTIMIENTO

El consentimiento es la manifestación de la voluntad libre, específica e informada del titular de los datos personales, que permite el tratamiento de su información personal; asimismo, el artículo 20 de la Ley General, señala que el responsable deberá contar con el consentimiento previo por parte de las personas titulares de la información personal, cumpliendo con las siguientes características:[18]

***Previo*:** Cuando los datos personales se obtengan de forma personal o directamente del titular.

Libre: Sin que medie error, mala fe, dolo o violencia que impidan al titular conocer los usos a que serán sometida su información personal y, en consecuencia, puedan afectar o viciar su manifestación de voluntad.

Específico: La autorización que se solicite debe estar vinculada a una o varias finalidades que motiven el tratamiento de los datos personales.

18 Artículo 20 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Informado: El titular tiene conocimiento del aviso de privacidad, previo a que sus datos personales sean tratados.

Cuando el titular deba otorgar ciertos datos personales al responsable, motivado por alguna situación de emergencia, éste ***deberá previamente otorgar su consentimiento***, más aún cuando se trata de facilitar los datos personales sensibles.

PROPORCIONALIDAD

En caso de que se solicitaran datos personales a las personas titulares en casos fortuitos o de fuerza mayor, se deberá prever qué datos son adecuados, relevantes y estrictamente necesarios para el cumplimiento de las finalidades que motivaron su obtención, para que en este caso no se soliciten datos de forma indiscriminada o excesiva, sino atendiendo al principio de proporcionalidad, datos que deberán guardar relación con los fines que legitiman el tratamiento.

INFORMACIÓN

El responsable deberá hacer del conocimiento a las personas titulares, previo a la solicitud de los datos personales, cuál será el tratamiento que se dará a los mismos, a fin de que las personas titulares puedan tomar decisiones informadas al respecto, y puedan ejercer su derecho a la protección de su información personal.

El responsable en cumplimiento al principio de información deberá informar al titular a través del aviso de privacidad, la existencia y características principales del tratamiento que se dará a los datos personales, el que deberá contener:

- Nombre y domicilio del responsable.
- Los datos personales que serán sometidos a tratamiento, identificando los datos personales sensibles.
- El fundamento legal que faculta al responsable para el tratamiento de los datos personales.
- Las finalidades del tratamiento distinguiendo aquellas que requieran el consentimiento del titular.
- Los mecanismos, medios y procedimientos para ejercer los derechos ARCO.
- Los mecanismos, medios y procedimientos para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales, para las finalidades y transferencias de datos personales que requieren el consentimiento del titular.
- El domicilio de la Unidad de Transparencia.
- Los medios por los cuales el responsable dará a conocer los cambios al aviso de privacidad.

Cabe resaltar que, con independencia que se requiera o no el consentimiento del titular para el tratamiento de sus datos personales, el responsable está obligado a poner a su disposición el aviso de privacidad, cuando se presente algún caso fortuito o de fuerza mayor, de acuerdo a los planes y programas de emergencia que al efecto emitan las autoridades competentes, se podrán requerir datos personales de las personas titulares que se encuentran en situación de vulnerabilidad por la situación de emergencia.

RESPONSABILIDAD

Con este principio se establece la obligación de los responsables de vigilar se cumplan los principios y deberes mediante los mecanismos que adopte para su aplicación; y que tengan como finalidad la protección de los datos personales.

La Ley General contempla, en su artículo 30, los mecanismos que el responsable debe adoptar para cumplir con este principio, y que a continuación se señalan:

- Instrumentar programas y políticas de protección de datos personales.
- Contar con políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable.
- Capacitar y actualizar al personal sobre las obligaciones y demás deberes en materia de protección de datos personales.

  Para lo que sugerimos a las personas titulares conocer la oferta de capacitaciones que ofrece el Centro Virtual de Formación INAI (CEVINAI) a través de su página de internet, disponible en el siguiente enlace: ***http://cevifaiprivada.ifai.org.mx/ swf/cevinaiv2/cevinai/index.php,*** con el objeto de que tenga conocimiento sobre las obligaciones y deberes en materia de protección de datos personales.
- Revisar y modificar periódicamente las políticas y programas de seguridad de datos.
- Comprobar el cumplimiento de las políticas de protección de datos personales a través de sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías.
- Establecer procedimientos para recibir y responder dudas y quejas de las personas titulares.
- Diseñar, desarrollar e implementar políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales en términos de la normatividad aplicable.
- Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en términos de la normatividad aplicable.

Adicional a lo antes señalado, los responsables competentes ante una situación de emergencia deberán vigilar que los datos recabados atiendan los principios antes señalados, a fin de evitar alguna vulneración más a las personas titulares de los datos.

Los responsables no deberán conservar los datos que hayan sido recabados de las personas titulares hasta el cumplimiento de los fines para los cuales fueron solicitados en una situación de emergencia, para lo que se sugiere a las personas titulares cerciorarse que en el aviso de privacidad se especifique el tiempo de conservación de sus datos personales.

TRANSFERENCIA O TRANSMISIÓN

En términos de lo dispuesto en la LGDPDPPSO transferencia es toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado[19]. Esta comunicación puede producirse, por el envío de los datos a un tercero, ya sea que físicamente le sean mostrados o se les permita el acceso a ellos a través de algún medio electrónico o plataforma digital. ***Toda transferencia requiere el consentimiento de su titular***.

La transferencia de datos personales puede ser:

- ***Nacionales***, dentro del territorio mexicano.

- ***Internacionales,*** fuera del territorio nacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, y serán posibles cuando el receptor de los datos personales asuma las mismas obligaciones que corresponden al responsable que transfirió los datos personales.

En ambos casos, es necesario que se cumpla con todos los principios y deberes de la protección de datos, que establece la Ley General y los Lineamientos Generales.

Adicional a lo anterior, los responsables que transfieren datos personales están obligados a formalizar la transferencia mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes, salvo en los siguientes casos:

- Cuando sea nacional y se realice en cumplimiento a una disposición legal o en el ejercicio de las facultades con que cuenta el transferente y receptor de los datos personales.

- Cuando sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.

El consentimiento deberá ser otorgado por el titular en el aviso de privacidad que al efecto ponga a disposición el responsable transferente, informándole el objeto de la transferencia o transmisión que se deberá limitar a la finalidad y condiciones informadas y consentidas, en su caso, en el aviso de privacidad. El responsable que transfiere los datos personales comunicará al responsable que recibe los datos personales, el aviso de privacidad correspondiente.

19 Artículo 3, fracción III de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Los sujetos obligados ***no requerirán el consentimiento de las personas titulares*** para realizar una transferencia o transmisión, en los siguientes casos:[20]

- Esté prevista en alguna ley, en convenios o Tratados Internacionales suscritos y ratificados por México;
- **Cuando se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales**;
- Cuando sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;
- Cuando sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;
- **Cuando sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados**;
- Cuando sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular;
- Cuando sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
- Cuando se trate de los casos en los que el responsable no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión o transferencia de sus datos personales, conforme a lo dispuesto en el artículo 22 de la LGPDPPSO, o
- **Cuando sea necesaria por razones de seguridad** nacional.

El responsable receptor tiene la obligación de tratar los datos personales de conformidad con lo establecido en el aviso de privacidad, debiendo limitar el tratamiento de los datos personales transferidos a las finalidades que justificaron las transferencias; asumir las mismas obligaciones que corresponden al responsable que transfirió los datos, cumpliendo con los principios y deberes que establece la LGPDPPSO.

Cuando se deba realizar alguna transferencia de datos personales en situaciones de emergencia se sugiere al responsable del tratamiento de los datos personales lo siguiente:

- Identificar las transferencias y/o transmisión de datos personales que se vayan a realizar en una situación de emergencia de datos personales, a fin de cumplir en todos los casos con las obligaciones antes descritas.
- Informar al titular de los datos personales a través del aviso de privacidad las transferencias que se realizarán, quien será el receptor y las finalidades de la transferencia.

20 Artículo 70 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

- Solicitar el consentimiento expreso y por escrito para transferir datos personales sensibles.

- No realizar transferencias de datos personales a terceros no autorizados por las personas titulares, salvo que se actualicen las excepciones previstas en los artículos 22 y 70 de la LGPDPPSO.

- Las transferencias y/o transmisión de datos personales que realicen los responsables a otras autoridades competentes deberán documentarse de manera clara, fundamentarse y efectuarse considerando medidas de seguridad que garanticen la protección de los datos personales.

- La transferencia y/o transmisión de datos personales se deberá realizar en cumplimiento de las disposiciones normativas en la materia, esto es a la LGPDPPSO, y a los Lineamientos Generales.

RECOMENDACIONES

Respecto a la protección de datos personales, en situaciones de emergencia se emiten las siguientes recomendaciones:

- Identifica los datos personales necesarios para la atención de la situación de emergencia.
- Cerciórate que el responsable esté facultado para atender la emergencia y, en consecuencia, para recabar los datos en la situación de emergencia, en medida de lo posible.
- Los datos personales solicitados deben ser acordes con los planes de emergencia y los programas de gestión del riesgo que emitan las autoridades al respecto.
- Tome en cuenta la información difundida por los responsables, a través de los medios de comunicación oficiales la información relativa al tratamiento de los datos personales en la situación de emergencia que se presente.
- Cuando exista una situación de emergencia que potencialmente le pueda dañar en su persona o en sus bienes, no se recabará su consentimiento. En el caso de tratamiento de datos personales sensibles en una situación de emergencia, sólo debe realizarse con su consentimiento expreso y por escrito del titular, a través de su firma, huella dactilar, firma electrónica o cualquier mecanismo de autenticación que se encuentre autorizado.
- En caso de que se vayan a realizar transferencias de sus datos personales, los responsables deberán hacerlo del conocimiento de las personas titulares, previa solicitud de su consentimiento, en este caso, se lo deben hacer saber al poner a su disposición el aviso de privacidad.
- Los responsables no podrán realizar transferencias de datos personales a terceros no autorizados por las personas titulares, salvo que se actualicen las excepciones previstas en los artículos 22 y 70 de la LGPDPPS.

DENUNCIAS

El tratamiento inadecuado o indebido de tus datos personales que cualquier sujeto obligado haya realizado puede ser denunciado ante el INAI; puedes acudir al Instituto a presentar tu denuncia presentando los siguientes requisitos:[21]

- El nombre de la persona que denuncia, o en su caso, de su representante;
- El domicilio o medio para recibir notificaciones de la persona que denuncia;
- La relación de hechos en que se basa la denuncia y los elementos con los que cuente para probar su dicho;
- El responsable denunciado y su domicilio, o en su caso, los datos para su identificación y/o ubicación;
- La firma o huella digital del denunciante, o en su caso, de su representante.

- Si la denuncia se presentó por escrito, ésta deberá contener la firma autógrafa del denunciante, a menos que no sepa o no pueda firmar, en cuyo caso imprimirá su huella digital.[22]

- Si la denuncia se presentó por medios electrónicos, ésta deberá incluir el documento digitalizado que contenga la firma autógrafa, o bien, la firma electrónica avanzada del denunciante o del instrumento que lo sustituya.[23]

La denuncia puede presentarse de manera presencial ante la Oficialía de Partes del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales con domicilio ubicado en Insurgentes Sur, número 3211, Colonia Insurgentes Cuicuilco, Delegación Coyoacán, C.P. 04530, en un horario de lunes a jueves de 9:00 a 18:00 horas y viernes de 9:00 a 15:00 horas, o si lo prefiere de manera electrónica al correo electrónico de la Dirección General de Investigación y Verificación del Sector Público: investigayverifica@inai.org.mx.

El INAI, pone a tu disposición un formato que te puede auxiliar en la elaboración de tu denuncia, mismo que puedes consultar a través del siguiente enlace: http://inicio.ifai.org.mx/FormatosINAI/FormatodenunciaLGPDPPSO.PDF

Asimismo, se le informa que el Instituto cuenta con un Centro de Atención a la Sociedad (CAS) que está a su disposición para darle asesoría y responder sus dudas previo a la presen-

21 Artículo 148 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

22 Al respecto, el artículo 192 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, señala que las denuncias no deben contener mayores requisitos que los previstos en el artículo 148 de la Ley referida con antelación; sin embargo, en la presentación de las denuncias se deberá observar dichos requisitos.

23 Ídem.

tación de la denuncia, en el teléfono 800 83 54 324, en un horario de lunes a jueves de 9:00 a 18:00 horas y viernes de 9:00 a 15:00 horas.

Adicionalmente a lo anterior, y para mayor información, se orienta a las personas Titulares que pueden ponerse en contacto con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, ubicado en Avenida Insurgentes Sur número 3211, Colonia Insurgentes Cuicuilco, Alcaldía Coyoacán, Código Postal 04530, en la Ciudad de México, de lunes a jueves, en un horario comprendido de las 9:00 a las 18:00 horas y los viernes, de 9:00 a 15:00 horas, en horario continuo, o bien, puede comunicarse al número telefónico gratuito 800 TEL INAI (800 835 4324) o al correo electrónico: atencion@inai.org.mx, donde con mucho gusto se le atenderá.


inai
Instituto Nacional de Transparencia, Acceso a la
Información y Protección de Datos Personales