

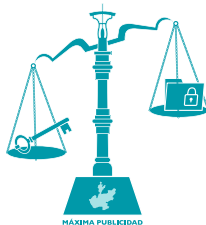
CURSO: INTRODUCCIÓN

A LA PROTECCIÓN
DE DATOS PERSONALES
EN POSESIÓN
DE SUJETOS OBLIGADOS
DEL ESTADO DE JALISCO

MANUAL DE PARTICIPANTE



INSTITUTO DE TRANSPARENCIA, INFORMACIÓN PÚBLICA
Y PROTECCIÓN DE DATOS PERSONALES
DEL ESTADO DE JALISCO



CESIP

Centro de Estudios Superiores de
la Información Pública y
Protección de Datos Personales

DIRECTORIO

INSTITUTO DE TRANSPARENCIA, INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE JALISCO (ITEI)

Salvador Romero Espinosa

Comisionado Presidente

Pedro Antonio Rosas Hernández

Comisionado Ciudadano

Ximena Guadalupe Raygoza Jiménez

Secretaria Ejecutiva

Manuel Rojas Munguía

Director del Centro de Estudios Superiores de la Información Pública y Protección de Datos Personales (CESIP)

INVESTIGACIÓN NORMATIVA Y ADAPTACIÓN PARA JALISCO A CARGO DEL CESIP:

Jessica Guadalupe Mejía Álvarez

Manuel Rojas Munguía

Carlos Alberto Barrera González

Rafael Amézquita Castellanos

Dirección de Vinculación y Difusión

Olga Navarro Benavides

Juan Francisco García Gallegos

"El presente manual fue elaborado en el año 2019 por el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México bajo la coordinación de la Dirección de Capacitación para la Cultura de la Transparencia, la Protección de Datos Personales y la Rendición de Cuentas y personal adscrito a la misma."

IMPRESO Y HECHO EN MÉXICO

Primera Edición Jalisco, Diciembre 2022



@ITEIJal



ITEIJal



iteijalisco



iteijalisco



@CESIP_ITEI

www.itei.org.mx



Av. Ignacio L. Vallarta 1312
Col. Americana, C.P. 44160
Guadalajara, Jalisco, México

CURSO: INTRODUCCIÓN

A LA PROTECCIÓN
DE DATOS PERSONALES
EN POSESIÓN
DE SUJETOS OBLIGADOS
DEL ESTADO DE JALISCO

MANUAL DE PARTICIPANTE



INSTITUTO DE TRANSPARENCIA, INFORMACIÓN PÚBLICA
Y PROTECCIÓN DE DATOS PERSONALES
DEL ESTADO DE JALISCO



CESIP

Centro de Estudios Superiores de
la Información Pública y
Protección de Datos Personales

Contenido

Presentación	1
1. Introducción	3
2. Objetivo del curso	4
3. Contenido del curso	4
3.1. Introducción al curso	4
3.1.1 Evaluación diagnóstica	5
3.2 Módulo 1. Conceptos y definiciones básicas	6
3.2.1 Evaluación formativa	13
3.3 Módulo 2. Evolución de la protección de datos personales en posesión de sujetos obligados en el Estado de Jalisco	14
3.3.1 Evaluación formativa	18
3.4 Módulo 3. Aspectos relevantes de la Ley de protección de datos personales en posesión de sujetos obligados del Estado de Jalisco	19
3.4.1 Evaluación formativa	34
4. Anexos	35
Anexo 1. APLICACIÓN DE LOS PRINCIPIOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE JALISCO	35
5. Bibliografía y referencias	36
Legislación local	36
Legislación nacional	36
Legislación internacional	37

Presentación

El Instituto de Transparencia, Información Pública y Protección de Datos Personales (ITEI), en su naturaleza de Organismo Garante, tiene la encomienda de ser un órgano revisor de las demás entidades de Estado y controlar su actuar para garantizar el ejercicio de los derechos fundamentales. En el caso de nuestro Instituto, la misión que cumple resulta prioritaria para lograr una gestión responsable e institucionalizada de las entidades estatales. Dicha misión es garantizar el ejercicio del derecho de acceso a la información pública, la rendición de cuentas, así como el uso adecuado de los datos personales.

Bajo ese tenor, el Instituto tiene la atribución de generar mecanismos de formación y concientización que facilite el cumplimiento de los objetivos institucionales que la sociedad jalisciense nos ha confiado. Ello implica que, de manera paralela a los mecanismos jurídicos que permiten vigilar a las instituciones y hacerles cumplir sus obligaciones en la materia, la Institución también puede establecer estrategias que capaciten a quienes ejercen el servicio público para prevenir infracciones en el cumplimiento de las obligaciones respecto al uso de datos personales. Ello, sin dejar de lado la importante labor de información a la ciudadanía para que pueda determinar el uso que se le da a su información, así como ejercer mecanismos de defensa a la protección de la misma.

Por ello, en aras de contribuir en dichas áreas de trabajo que desarrolla este Organismo, se

presenta este documento. Este manual, junto a la serie de materiales que le acompañan, representa un esfuerzo interinstitucional por reforzar los conocimientos en materia de protección a la intimidad y la información personal de las y los ciudadanos. Ello, desde dos líneas distintas, por un lado, se busca que la sociedad cuente con dichos conocimientos para que haga uso de ellos y defienda su información. En un segundo momento, igualmente importante, es para que las y los servidores públicos del Estado cumplan con las responsabilidades en estas materias.

Este manual posee tintes estrictamente pedagógicos, introductorios e integrales, busca capacitar de manera general a las personas participantes sobre las obligaciones que tienen los sujetos obligados respecto el manejo de la información de las personas, la manera controlar que dicha obligaciones sean cumplidas, los mecanismos para proteger los datos personales en caso de que se estén usando de manera indebida, así como ejercer mecanismos de defensa ante infracciones o malas prácticas institucionales.

Sin duda, la variedad de manuales que hoy pone el ITEI a disposición de la sociedad y de las instituciones jaliscienses es gracias a la colaboración interinstitucional con el INFOCDMX a quienes agradezco su compromiso con la formación continua como el mejor mecanismo para fortalecer la gobernanza institucional y la participación ciudadana.

Enhorabuena a quienes hoy tienen la oportunidad y la disposición de capacitarse en este tema. Sin duda, este material será de gran ayuda para el ejercicio de la función pública y el desarrollo profesional dentro de las instituciones. Reitero mi alegría al presentar este libro, deseando la mejor de las experiencias.

Mtro. Pedro Antonio Rosas Hernández
Comisionado Ciudadano del ITEI

1. Introducción

En cumplimiento de las atribuciones en materia de capacitación con que cuenta el Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI), el Centro de Estudios Superiores de Información Pública y Protección de Datos Personales (CESIP), presenta este manual. El objetivo de este esfuerzo es dotar de herramientas que respalden a las habilidades pedagógicas de quienes se dedican a la capacitación, formación y sensibilización en materia de protección de datos personales y la gestión de los mismos. Así mismo, también tiene el objetivo de estandarizar la calidad pedagógica de las capacitaciones a fin de propiciar el máximo aprovechamiento por parte de las personas que participen en dichas capacitaciones. Por tanto, este manual es una contribución significativa para el robustecimiento de una efectiva cultura de los derechos humanos en nuestro Estado y en nuestro país.

El programa de capacitación sobre el que se construye el manual fue realizado en primera instancia por personal del INFOCDMX (adaptado a Jalisco por el CESIP) y se integra por tres módulos. En el primero se da un panorama amplio y general respecto a la protección de datos personales como una prerrogativa que el ITEI (y el Sistema Nacional de Transparencia) debe proteger, así como una introducción a los conceptos necesarios para familiarizarse a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios. En el segundo módulo se habla de manera específica sobre la protección de datos personales y sus antecedentes en el Estado de Jalisco y en México.

Finalmente, se hace un análisis detallado sobre el contenido de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios. Al finalizar este último módulo, las personas participantes conocerán los principios y deberes que deben ser observados por los sujetos obligados, los derechos de la ciudadanía respecto al manejo de sus datos personales, las capacidades del ITEI en la materia, los procesos de solicitudes de derechos ARCO así como los procedimientos de impugnación en la materia, las medidas de apremio y las sanciones.

Ahora bien, es momento de iniciar con el contenido formativo del manual. Me despido, no sin antes agradecer a todos los esfuerzos y colaboraciones que han hecho posible la elaboración y publicación de este valioso material de capacitación.

Mtro. Manuel Rojas Munguía

Director del Centro de Estudios Superiores
de Información Pública y Protección de Datos
Personales

2. Objetivo del curso

El participante al final del curso identificará los aspectos principales del derecho de la protección de datos personales, así como de la Ley Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, a través de la exposición y análisis de diversos conceptos y definiciones relevantes de la ley de protección de datos local, con la finalidad de tomar conciencia de las implicaciones que tienen en la vida cotidiana y en labores diarias de cada persona.

Se identificarán los principios, conceptos básicos, obligaciones y deberes establecidos en la Ley Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios (Ley de datos local), además de que desarrollarán empatía y sensibilidad en temas de intimidad, privacidad y el derecho a la protección de datos personales en aras de garantizar este derecho humano en el ejercicio de la función pública, en beneficio de la sociedad en su conjunto.

Lo anterior, dado que, para el caso de los servidores públicos, resulta indispensable observar el derecho a la protección de datos personales desde dos perspectivas: como un deber institucional y como una prerrogativa como individuo; perspectivas que, al ser asimiladas en conjunto.

Facilitarán el entendimiento y su aplicación cotidiana en las actividades que desarrollan, en el ámbito institucional, e incluso, al impulsar su mejora.

3. Contenido del curso

3.1. Introducción al curso

El curso se conforma por 3 módulos, cuyo orden facilita la identificación de conceptos y principios, la evolución de la protección de datos personales en posesión de sujetos obligados en el Estado de Jalisco y los aspectos principales en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Con el desarrollo de cada uno de los módulos, se busca conseguir los siguientes objetivos:

Módulo 1. Conceptos y definiciones básicas. Identificar de los conceptos y definiciones básicas aplicables a la protección de datos personales, tales como la privacidad e intimidad; e incluye los conceptos que enuncia la propia Ley de datos local.

Módulo 2. Evolución de la Protección de Datos personales en posesión de sujetos obligados en el Estado de Jalisco. Tomar conciencia de la evolución histórica y normativa del derecho a la protección de datos personales en la entidad federativa.

Módulo 3. Aspectos relevantes de la Ley. Identificar los aspectos relevantes de la Ley de Protección de Datos Personales local, con la finalidad de asimilar las implicaciones que tiene en las labores diarias dentro de los sujetos obligados del Estado de Jalisco.



3.1.1 Evaluación diagnóstica

Antes de dar inicio al estudio del primer módulo, se invita a reflexionar, y anotar sus ideas, en torno a los siguientes cuestionamientos:

1. ¿Qué piensan cuando escuchan el término Datos Personales?

2. ¿Son importantes los datos personales?

3. ¿Cómo protegemos los datos personales?

3.2 Módulo 1. Conceptos y definiciones básicas

En este módulo se abordarán los conceptos y definiciones básicas aplicables a la materia de protección de datos personales en posesión de sujetos obligados, con la finalidad de que los participantes identifiquen cada uno de ellos y los sitúen en sus actividades cotidianas, es decir, se debe buscar que los participantes generen conciencia de que el servicio público está sujeto a las reglas dispuestas para la protección de datos personales, a partir de conceptos que se ven materializados día con día. Por ello, resulta necesario exponer cada uno de los principales conceptos.

El objetivo de este módulo es **identificar** los conceptos y definiciones básicas aplicables al derecho de la protección de datos personales con la finalidad de reconocer los aspectos relevantes de la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

Intimidad

Lo «íntimo» podría pensarse como el ámbito tanto de los pensamientos de cada cual, de la formación de decisiones («lo aún no expresado y que probablemente nunca lo será»), como de aquellas acciones cuya realización no requiere la intervención de terceros y tampoco los afecta.¹

Dentro de este ámbito pueden pensarse aquellas acciones autocentradas en el individuo. La intimidad es la parte más personal o lo reconocido como lo más recóndito del ser, es aquello que queda fuera de cualquier injerencia, sólo le pertenece a la persona, no se exterioriza, es su esfera espiritual, moral.



«La intimidad es el sinónimo de conciencia, de vida interior»

Recaséns Siches.



Lecturas recomendadas

- García Ricci, Diego, El derecho a la privacidad, Nostra Ediciones, 2017.
- Criterios del Poder Judicial de la Federación: en materia de protección de datos personales y otros conceptos relacionados, SCJN, 2018.

Privacidad

En el ámbito de lo «privado» se requiere necesariamente, a diferencia de lo íntimo, la presencia de por lo menos dos actores. Se trata del ámbito donde pueden imperar exclusivamente los deseos y preferencias individuales, como condición necesaria para el «ejercicio» de la libertad individual,

¹ Garzón Valdés, Ernesto, Lo íntimo, lo privado y lo público, Cuadernos de Transparencia # 6, INAI, 2015.

conformando así la «esfera personal reconocida».

Es el ámbito de nuestra vida como individuos que dejamos fuera del escrutinio público. Es parte de nuestra autodeterminación informativa, y es importante su protección, ya que en todo momento se puede ver afectado por un tercero o por el gobierno. En el contexto actual, el poder económico, social y político se obtiene en primera instancia del control de la conducta de los individuos, por ello la protección a la privacidad de los individuos es una necesidad primordial de las sociedades actuales.

Derecho a la privacidad

Es una prerrogativa que todo individuo tiene a separar aspectos de su vida privada del escrutinio público.² Tiene dos componentes, el primero de ellos, es el que tiene el individuo de aislarse; lo cual permite poner una barrera y limitar el acceso de miramientos ajenos no consentidos. El segundo componente, es aquel referido al control que se tiene de la información propia. La privacidad vista como un derecho que se debe respetar, para garantizar la libertad y tener el control sobre quienes conocen y hasta donde conocen sobre la información de cada individuo.

Es una condición necesaria para el ejercicio de la libertad individual y constituye una “esfera personal reconocida” en la que se reserva un tipo de situaciones o relaciones interpersonales en donde la selección

de los participantes depende de la libre decisión de cada individuo.³ Este derecho esta salvaguardado en el primer párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, la SCJN señala que la garantía de seguridad jurídica, «puede extenderse a una protección que va más allá del aseguramiento del domicilio como espacio físico en que se desenvuelve normalmente la privacidad»⁴ Aunado con el derecho a la autodeterminación informativa, el único dueño de la información relativa al individuo es éste. El derecho a la privacidad es la base de la protección de los datos de carácter personal, ya que al proteger éstos se protege la privacidad de los individuos.



Lecturas recomendadas

- Garzón Valdés, Ernesto, Lo íntimo, lo privado y lo público, Cuadernos de Transparencia # 6, INAI, 2015, disponible en: <http://inicio.ifai.org.mx/PublicacionesComiteEditorial/Cuadernillo%2006%20B.pdf>
- Gonzalbo, Escalante Fernando, El derecho a la privacidad. Cuadernos de Transparencia # 2, INAI, 2015, disponible en: <http://inicio.ifai.org.mx/PublicacionesComiteEditorial/Cuadernillo%2002%20B.pdf>

² García Ricci, Diego, Artículo 16 Constitucional. Derecho a la privacidad, IJ-UNAM, 2013.

³ Tenorio Cueto, G. A. et al. Los Datos Personales en México. Perspectivas y Retos de su Manejo en Posesión de Particulares, México: Editorial Porrúa, 2012.

⁴ 1 69700. 2a. LXIII/2008. Segunda Sala. Novena Época. Semanario Judicial de la Federación y su Gaceta. Tomo XXVII, mayo de 2008, Pág. 229

Datos Personales

Un dato es un antecedente para llegar al conocimiento de algo⁵, es un elemento material susceptible de convertirse en información y de igual manera de ser transferido y reunido de manera sistemática.

La información de una persona representada en datos personales revela gustos, preferencias, ideologías, pensamientos, es decir, todo aquello que nos constituye como individuos. Los datos personales son cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente.

Datos Personales Sensibles

Los datos personales sensibles son aquellos que afectan directamente al desarrollo de la persona y tienen un potencial de daño para éstas, lo cual puede ser determinado por el contexto social, cultural y en última instancia por la ley.

Los datos sensibles son, entre otros:

- Datos ideológicos
- Datos de salud
- Características personales (datos biométricos)
- Preferencia sexual
- Características físicas (color de piel, estatura, peso, discapacidades)

Por regla general no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento previo, expreso, informado e inequívoco de su titular.

La utilización de los datos personales indebida puede dar origen a discriminación o conllevar un riesgo grave para la seguridad de su titular, ya que puede lesionar sus derechos. Los datos con estas características tienen una mayor protección en las distintas legislaciones.

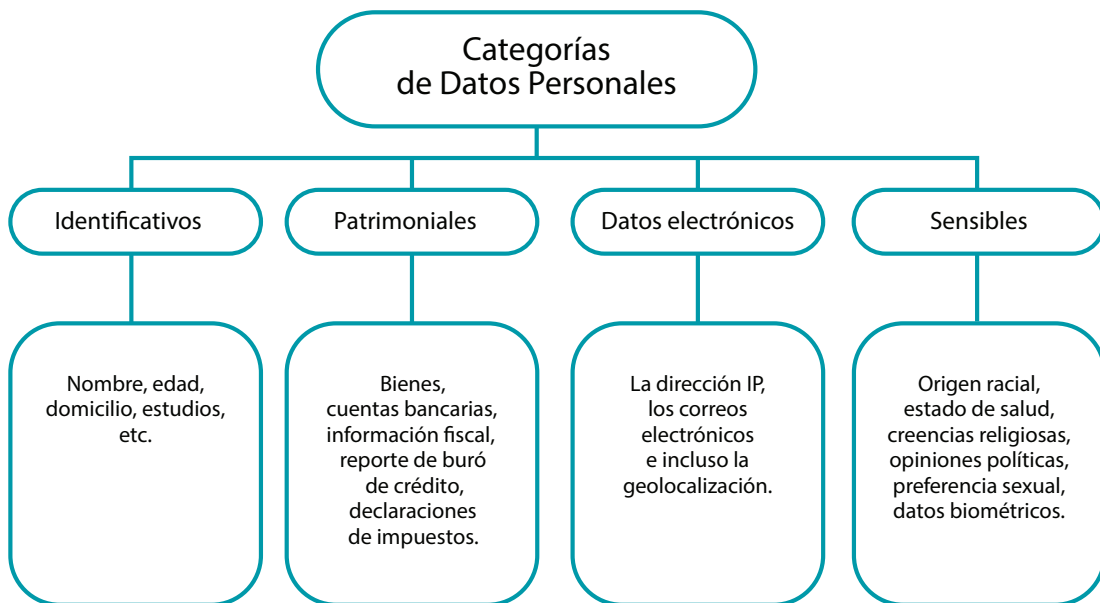
Datos Personales de Menores de Edad

Si bien, la distinción más conocida en las normas de datos es relativa a los datos sensibles, hay que tener en cuenta que el tratamiento de datos personales relativo a menores de edad debido a su condición de vulnerabilidad deben ser tratados de una forma específica ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales, y siempre tomado en consideración el principio del interés superior de menor.

⁵ Dato: www.rea.es

Categorías y Tipos de Datos

En las legislaciones que regulan la protección de datos personales, en particular, aquellas que aclaran su aplicabilidad, a través de lineamientos o reglamentos señalan diversas categorías y tipos de datos personales, más allá de la distinción que se hace respecto a los datos sensibles.



¿Por qué proteger los datos personales?

La autodeterminación informativa es el reconocimiento al individuo de la facultad de disposición y decisión respecto a sus propios datos personales. Este derecho, reconoce al sujeto la facultad de decidir cuándo y cómo está dispuesto a permitir que se difunda su información personal o a difundirla él mismo.

La protección de datos personales es una prerrogativa que tiene el titular de los datos para proteger cualquier información concerniente a su persona.

La protección de la intimidad, privacidad y autodeterminación informativa al igual que el derecho a la protección de datos personales buscan procurar la dignidad de las personas.



Tratamiento de datos personales

El término “Tratamiento de datos personales” refiere a cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionados con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, etc.



Es legítimo si cumple con:

- Principios

El responsable debe contar con:

- Aviso de privacidad
- Registro del (los) sistema (s) de datos personales
- Documento de Seguridad

Este tratamiento requerirá el consentimiento inequívoco, expreso y por escrito del interesado, salvo en los casos y excepciones previstas en la Ley.

El tratamiento de los datos personales inicia al momento en que se recaban por primera vez los datos personales, sin embargo, el tratamiento también implica, entre otras situaciones: gestión de personal y administración de nóminas; acceso o consulta

a bases de datos de contactos que contengan datos personales, almacenamiento de direcciones IP o MAC; grabación de vídeo.

Los sistemas de datos personales que hayan sido objeto de tratamiento deberán ser suprimidos una vez que concluyan los plazos de conservación establecidos por las disposiciones aplicables, o cuando dejen de ser necesarios para los fines por los cuales fueron recabados.

Sistema de Datos personales

Este término se refiere al conjunto organizado de archivos, registros, ficheros, bases o bancos de datos personales en posesión de los sujetos obligados. Los sistemas de datos personales tienen como finalidad cumplir con la transparencia, responsabilidad, y licitud en el tratamiento de datos personales.

El registro de los sistemas de datos personales de los sujetos obligados debe contemplar como mínimo:

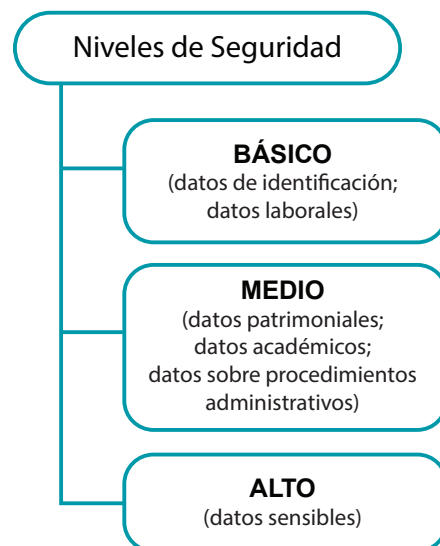
- Nombre y cargo del titular del sujeto obligado como responsable del tratamiento y los usuarios.
- Finalidad o finalidades del tratamiento.
- Naturaleza de los datos personales contenidos en cada sistema.
- Formas de recabación, pertinencia, proporcionalidad y calidad de datos.
- Las posibles transferencias.
- Modo de interrelacionar la información registrada.
- Ciclo de vida de los datos personales y tiempos de conservación, y
- Medidas de seguridad.

Queda prohibida la creación de sistemas de datos personales que tengan como finalidad exclusiva tratar datos sensibles. Estos datos sólo podrán tratarse cuando medien razones de interés general, así lo disponga una ley, haya un consentimiento expreso o con fines estadísticos o históricos.

Medidas de seguridad

Son el conjunto de acciones, actividades, controles o mecanismos administrativos, **técnicos y físicos que permiten** proteger los datos personales y los sistemas de datos personales.

Los niveles de seguridad responden a la mayor o menor necesidad de garantizar la integridad de los datos personales. Por lo tanto, las dependencias y entidades aplicarán el nivel básico, medio o alto de medidas de seguridad, de conformidad al tipo de datos personales recabados.



Titular

La persona física a quien corresponden los datos personales, y como tal sólo éste podrá tener acceso a su información.

Responsable

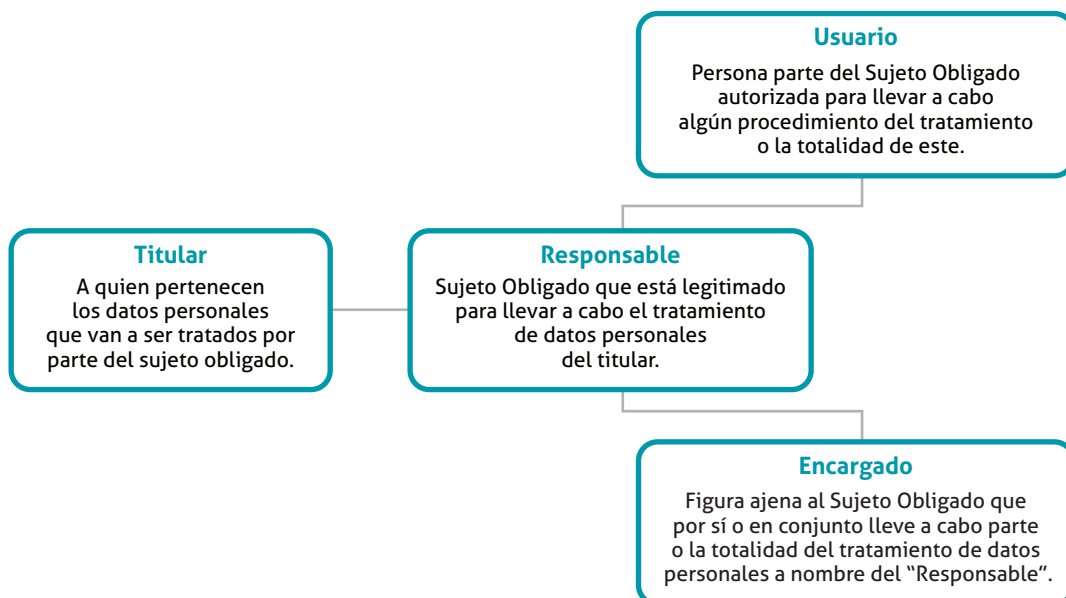
Cualquier sujeto obligado que decida y determine la finalidad, fines, medios, medidas de seguridad y demás cuestiones relacionadas con el tratamiento de datos personales. El responsable determinará el tratamiento y todo lo concerniente a éste, de conformidad con sus atribuciones legales.

Usuario

Persona autorizada por el responsable e integrante del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o sistema de datos personales.

Encargado

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





3.2.1 Evaluación formativa

Concluido el primer módulo, se sugiere contestar y reflexionar sobre las siguientes preguntas con la finalidad de reforzar la identificación de los conceptos básicos en materia de protección de datos personales.

1. ¿Qué información se encuentra en el ámbito íntimo y privado, cuál es la diferencia entre uno y otro?

2. ¿Qué importancia tiene la protección de la privacidad?

3. ¿A través de qué se expresa la privacidad de las personas?

4. ¿Por qué diferenciamos los datos personales sensibles?

5. ¿Cuáles son las figuras que participan de la protección de datos personales en los sujetos obligados?

3.3 Módulo 2. Evolución de la protección de datos personales en posesión de sujetos obligados en el Estado de Jalisco

En este módulo, el instructor abordará la evolución histórica y normativa del derecho de protección de datos personales en el Estado de Jalisco, con la finalidad de que se comprenda la protección de los datos personales como un derecho humano que deben garantizar los sujetos obligados del Estado de Jalisco, así como la importancia de la participación ciudadana y del establecimiento de una cultura de protección a los datos personales en las instituciones de la entidad.

El objetivo particular de este módulo es **tomar conciencia** de la evolución histórica y normativa de la protección de datos personales en Jalisco con la finalidad comprender el proceso de la cultura de protección de datos personales en posesión de sujetos obligados de la capital del país en el ámbito de sus labores diarias.

2002

Desde 2002 en México se reguló en la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental la protección de datos personales, sin embargo, ésta fue tratada particularmente a la luz de la transparencia y acceso a la información en los entes públicos. Lo dispuesto sobre el tema se encontraba en el Capítulo IV titulado Datos personales que incluía 6 artículos que regulaban de manera muy amplia la posesión

de datos personales por parte de los sujetos obligados en el ámbito federal.

Asimismo, se regularon los casos cuando se presentaba una confrontación con el derecho de acceso a la información, conocida como una excepción a la información pública: clasificación como confidencial, y el ejercicio de los derechos de acceso y rectificación de los datos personales.

Texto original de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

http://www.diputados.gob.mx/LeyesBiblio/abro/lftaipg/LFTAIPG_orig_11jun02.pdf

2002

En 2002 se publicó la Ley de Transparencia e Información Pública del Estado de Jalisco y sus Municipios, la cual, a diferencia de la lógica de la ley federal, no consideraba ningún tipo de disposiciones (ni siquiera amplias y breves, como en el caso federal) en torno a la protección de datos personales.

2007

El artículo 6º constitucional desde 1977 adoptó la garantía del derecho a la información señalando que éste será garantizado por el Estado; sin embargo, no existían los mecanismos correspondientes en leyes secundarias para garantizar este derecho, por lo cual, sólo quedaba como una declaración en

el texto constitucional.

A través de diversas iniciativas legislativas se presentaron proyectos para modificar disposiciones de la Constitución Política de los Estados Unidos Mexicanos, para dar lugar a la consolidación constitucional del derecho de acceso a la información.

El 20 de julio de 2007 se adicionó un segundo párrafo mediante una reforma constitucional al artículo 6º de la Constitución nacional, con lo cual se consolidó constitucionalmente la garantía del derecho de acceso a la información y en este contexto; la protección a la vida privada, los datos personales, los derechos de acceso y rectificación de datos personales y la creación de organismos garantes a nivel federal y estatal.

PROCESO LEGISLATIVO DE LA REFORMA CONSTITUCIONAL ARTÍCULO 6º

- 2006 (nov-dic) se presentaron diversas iniciativas de los grupos parlamentarios en la Cámara de Diputados.
- 2007 (marzo) Se presentó un dictamen por parte de las comisiones unidas de Puntos Constitucionales; y de la Función Pública, con proyecto de decreto que reforma el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos. Este dictamen fue aprobado y turnado a la Cámara de Senadores.
- 2007 (abril) Se presentó el dictamen en la Cámara de Senadores por parte de las Comisiones Unidas de Puntos Constitucionales; y de Estudios Legislativos, Segunda, con proyecto de decreto que adiciona un segundo párrafo con siete fracciones al artículo 6º de la Constitución Política de los Estados Unidos Mexicanos. Este dictamen fue aprobado y turnado a las legislaturas locales.
- 2007 (junio) Se reciben comunicaciones de voto aprobatorio de 17 legislaturas locales, por lo cual, queda aprobada la reforma y se envía para su publicación en el Diario Oficial de la Federación (DOF).
- 20 de julio de 2007 se publica la Reforma constitucional en el DOF al artículo 6º constitucional, adicionado un segundo párrafo.

Proceso completo de la reforma cons- titucional:
http://www.diputados.gob.mx/LeyesBiblio/proceso/lx/037_DOF_20jul07.pdf

2009

El 1 de junio de 2009 se publicó en el Diario Oficial de la Federación (DOF) la reforma al artículo 16 Constitucional, mediante la cual se adicionó un segundo párrafo, con el que se incluye la protección constitucional de datos personales y los derechos: de Acceso, Rectificación, Cancelación y Oposición (ARCO).

Con esta reforma constitucional y con la del artículo 73 constitucional, se arraigó la garantía del derecho a la protección de datos personales, a través del reconocimiento del habeas data, y es posible regular la protección de los datos personales en el ámbito particular.

2010

Ley Federal de Protección de Datos Personales en Posesión de Particulares es la primera ley nacional en regular la protección de los datos personales en posesión de los particulares que recopilan y tratan datos personales.

La finalidad de esta ley es regular el tratamiento legítimo, controlado e informado de los datos personales a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

2011

El Congreso del Estado de Jalisco aprueba la Ley de Información Pública del Estado de Jalisco y sus Municipios donde se recopilan disposiciones diversas respecto a la protección de datos personales.

2014

Desde 2002, con la publicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, se instauró el organismo garante del acceso a la información y protección de datos personales se consolidó en 2007 con la reforma constitucional al artículo 6º, se ampliaron sus atribuciones en 2010 en materia de datos personales en posesión de particulares y en 2014 se aprobó una reforma constitucional al artículo 6º, con la cual se ampliaron aún más las atribuciones del organismo garante nacional y de los organismos locales en materia de acceso a la información y protección de datos personales, estos últimos únicamente en el ámbito público.

PUNTOS RELEVANTES DE LA REFORMA 2014

- Se otorgó autonomía plena al organismo garante, ahora llamado: Instituto Nacional de Acceso a la Información y Protección de Datos Personales
- El pleno del INAI se conforma por 7 comisionados/as
- El INAI se constituye en una segunda instancia para resolver recursos de revisión, lo cual implica hacer una revisión de lo resuelto por los organismos garantes locales.
- Se amplió el catálogo de sujetos obligados
- El INAI como organismo garante deberá coordinar sus labores con otras instancias en aras de consolidar un sistema de rendición de cuentas.

2017

Derivado de la reforma de 2014, en 2017 se aprobó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, con la cual se establece el mínimo de protección de datos personales que deben seguir los sujetos obligados (del ámbito público) a nivel nacional, esto quiere decir que, a pesar de que las entidades están facultadas para emitir sus leyes en la materia, éstas no podrán ir más allá de lo dispuesto por la ley general, salvo cuando se dé un mayor beneficio a las personas, favoreciendo la protección más amplia en todo momento, para proteger y garantizar los derechos humanos conforme a los principios de universalidad, interdependencia, indivisibilidad y progresividad.

2017

A tenor de los nuevos cambios legislativos en materia de protección de datos personales, el Congreso del Estado de Jalisco aprueba la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, donde se siguen los lineamientos y lo dispuesto dentro de la ley general.

Los sindicatos y personas físicas y morales que manejen o reciban y ejerzan recursos públicos NO SON SUJETOS OBLIGADOS en esta Ley, son sujetos responsables en la Ley Federal de Protección de Datos Personales en Posesión de Particulares cuya observancia verifica el INAI.



3.3.1 Evaluación formativa

Concluido el segundo módulo se contestarán los siguientes cuestionamientos, lo anterior, servirá para precisar algunos de los temas desarrollados en este apartado.

1. ¿Qué artículos constituciones se han reformado para dar lugar a la protección de los datos personales en posesión de sujetos obligados?

2. ¿Qué importancia tiene el organismo garante nacional en el Estado de Jalisco?

3. El ITEI es el organismo garante local en material de protección de datos personales en posesión de sujetos obligados, ¿conocen quiénes son sus sujetos obligados?

3.4 Módulo 3. Aspectos relevantes de la Ley de protección de datos personales en posesión de sujetos obligados del Estado de Jalisco

En este módulo, el instructor o instructora llevará a los y las participantes a la identificación de los aspectos relevantes Ley de datos local, como son su objeto, principios, actores, obligaciones y procedimientos. El objetivo particular de este módulo es **identificar** los aspectos relevantes Ley Protección de Datos Personales en Posesión de Sujetos Obligados de Jalisco, con la finalidad de asimilar las implicaciones que tiene en las labores diarias dentro de los sujetos obligados del Instructor.

Principios y deberes

La aplicación de la ley de datos personales en posesión de sujetos obligados tiene como parte total los principios y deberes que no pueden dejar de observarse al momento de tratar datos personales. Los principios marcan los mínimos que las autoridades deben cumplir en un adecuado tratamiento de datos personales; ninguno de estos es optativo, así que en cada momento se debe velar por su cumplimiento, salvo las excepciones que la propia ley tiene establecidas. Cabe destacar que los principios no sólo se encuentran enunciados en las leyes nacionales o locales en México, ya que, al ser parte fundamental para la protección de datos personales, han sido adoptados por diversos instrumentos jurídicos internacionales, los cuales sirvieron de modelo para la regulación en México.

En el ámbito regional, México forma parte de la **Red Iberoamericana de Protección de Datos Personales (REIP)**, la cual busca que los Estados Iberoamericanos puedan adoptar y desarrollar su legislación nacional, con la finalidad de garantizar un debido tratamiento de los datos personales y contar con reglas homogéneas en la región.

Lo anterior, se expresa en los **Estándares de Protección de Datos Personales para los Estados Iberoamericanos**, los cuales pueden ser consultados en: http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf

En este documento se pueden observar los principios que la Ley de Jalisco, al igual que la General adopta.



Arts. 9-29
LPDPPSOEJ

PRINCIPIOS

Algunos de ellos son:

Calidad

Se requiere que el responsable adopte medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

Se presume que se cumple con el principio de calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.

Criterio de minimización

El responsable procurará realizar esfuerzos razonables para tratar los datos personales al mínimo necesario, con relación a las finalidades que motivan su tratamiento.

Consentimiento

Manifestación de la voluntad libre, específica e informada del titular de los datos personales, mediante la cual autoriza el uso de sus datos para su tratamiento.

El derecho fundamental a la protección de datos personales implica el control que el titular de los datos tiene sobre los mismos (autodeterminación informativa), por lo cual, la trascendencia de este principio es fundamental, y se vincula con el principio de información, ya que para que el titular pueda otorgar su consentimiento de manera informada, requiere que el responsable le informe todos los pormenores del tratamiento de los datos personales.

El consentimiento puede darse de manera tácita, salvo cuando se tratan datos personales sensibles, en este caso el consentimiento debe ser expreso, y en estos términos el responsable deberá facilitar un medio sencillo para poder otorgarlo.

El responsable tendrá la carga de la prueba en cuanto a demostrar que se obtuvo de manera adecuada el consentimiento para el tratamiento.

Excepciones a los principios de protección de datos personales:

Los principios no son absolutos, y las normativas específicas van marcando las excepciones a éstos, a grandes rasgos son aquellas que buscan proteger un bien común mayor o a la persona titular de los datos personales en su vida, dignidad o salud.

Consentimiento y los datos sensibles

En los *Estándares de Protección de Datos para los estados Iberoamericanos* se establece la siguiente regla:

Por regla general, el responsable no podrá tratar datos personales sensibles, salvo que se presente cualquiera de los siguientes supuestos:

- a. Los mismos sean estrictamente necesarios para el ejercicio y cumplimiento de las atribuciones y obligaciones expresamente previstas en las normas que regulan su actuación.
- b. Se dé cumplimiento a un mandato legal.
- c. **Se cuente con el consentimiento expreso y por escrito del titular.**
- d. Sean necesarios por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros.

Las excepciones al consentimiento están enunciadas en el artículo 15 de la LPDPPSOEJ

I. 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;

II. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;

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

IV. Cuando los datos personales sean necesarios en la atención de algún servicio sanitario de prevención o diagnóstico;

V. Cuando los datos personales figuren en fuentes de acceso público;

VI. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;

VII. Cuando los datos personales se sometan a un procedimiento previo de disociación;

VIII. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;

IX. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia; o

X. 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.

Finalidad

Los datos personales recabados y tratados tendrán fines determinados, explícitos y legítimos y no podrán ser tratados ulteriormente con fines distintos para los que fueron recabados. Datos sólo serán tratados para el fin o finalidades que se informaron al titular de los mismos para su tratamiento, de manera tal que si se pretende hacer uso de los datos con fines distintos al originario o será necesario obtener de nueva cuenta el consentimiento del titular.

La finalidad o finalidades deben ser determinadas y ajustadas a las atribuciones y facultades de los sujetos obligados.

El aviso de privacidad será el documento mediante el cual se solicitará el consentimiento al titular de los datos por parte de los sujetos obligados.

Aviso de privacidad

Es el documento a disposición del titular de los datos personales ya sea físico, electrónico o en cualquier formato generado por el responsable, con el objeto de informarle sobre la finalidad del tratamiento, así como la posibilidad de ejercer sus derechos ARCO (acceso, rectificación, cancelación y oposición).

Requisitos del aviso de privacidad: La identificación del responsable y la ubicación de su domicilio.

Fundamento legal que le faculta realizar el tratamiento de datos personales.

Enunciación de los datos a recabar.

El fin o finalidades del tratamiento

Información

El Responsable deberá informar al titular de los datos personales sobre las características principales del tratamiento, la finalidad y cualquier cambio del estado que guardan relacionados con sus datos personales.

Este principio se expresa en el “aviso de privacidad”, mediante el cual informa al titular sobre el tratamiento y todo lo concerniente a éste de conformidad con la normatividad vigente.

Lealtad

El tratamiento de datos personales se realizará sin que medie dolo, engaño o medios fraudulentos, tengan un origen lícito, y no vulneren la confianza del titular.

Licitud

Será lícito el tratamiento de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones que la normatividad aplicable les confiera y deberán obtenerse a través de los medios previstos en dichas disposiciones.

Proporcionalidad

El Responsable tratará aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con la finalidad, para la cual se obtuvieron, y sólo deberá recabar aquellos que resulten necesarios para la finalidad que justifique el tratamiento.

Se debe aplicar un criterio de minimización, el cual consiste en que el responsable deberá realizar los esfuerzos razonables para tratar los menos datos personales posibles en atención a su fin o finalidades.



**Arts. 30-44
LPDPPSOEJ**

Deberes

Los sujetos obligados que derivado de sus atribuciones realicen tratamiento de datos personales, a través de su responsable tienen, entre otros, los siguientes deberes en cumplimiento con las leyes específicas:

Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá garantizar las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

La confidencialidad es un deber fundamental, por lo cual, el responsable deberá establecer los mecanismos que tenga por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales (responsable, usuario y/o encargado), guarden la confidencialidad respecto a éstos, para poder

establecer políticas internas de cuidado de la infraestructura.

(Anatomía del Aviso de Privacidad, Ver Anexo 1)

Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

Un sistema de gestión es un conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

Derechos de los titulares y su ejercicio: Derechos Acceso, Rectificación, Cancelación y Oposición (ARCO)

Derivado de la prerrogativa que el titular de los datos personales tiene de mantener el control sobre estos, surgieron los ahora conocidos como derechos ARCO, mediante los cuales se garantiza que el titular de datos personales para acceder en cualquier momento a los mismos, rectificarlos, cancelarlos u oponerse a su uso.

Para el ejercicio de los derechos ARCO se requiere:

Que el titular acredite su identidad.

En caso de que sea un representante, quien vaya a ejercer los derechos, éste deberá acreditar la identidad y personalidad con la que actúa mediante una carta poder simple suscrita por dos testigos.

En caso de menores de edad, el ejercicio de los derechos será a través de padre, madre o tutor

En caso de personas fallecidas, el ejercicio de los derechos ARCO lo podrá realizar, la persona que acredite un interés jurídico o legítimo.

El ejercicio de estos derechos no es absoluto, ya que por razones previstas por ley pueden ser restringidos (. v.g. orden público, interés general)



Art. 61
LPDPPSOEJ

La presentación de solicitudes ARCO es gratuita, sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío, conforme a la normatividad que resulte aplicable. La información deberá ser entregada sin costo cuando implique la entrega de no más de veinte hojas simples, aunque se puede exceptuar el pago de reproducción y envío de acuerdo a las condiciones socioeconómicas del titular.

El ejercicio de estos derechos deberá ser sencillo, gratuito y el o la titular tendrá que acreditar la titularidad de los datos personales que pretende controlar, en caso de que se realice por un representante legal del o la titular, éste deberá estar debidamente acreditado.

El responsable no podrá establecer para la presentación de las solicitudes de derechos ARCO algún servicio o medio que implique un costo al o la titular.



Art. 46
LPDPPSOEJ

Derecho de Acceso

El derecho de Acceso se ejerce por el o la titular o su representante, para obtener y conocer la información relacionada con el uso, registro, fines, organización y conservación de sus datos personales, es una puerta de entrada para conocer con qué información (datos personales) concierne a él/ella cuenta algún sujeto obligado.

El principio de información es de suma importancia, ya que en el ejercicio de este derecho el o la titular tiene derecho para acceder a sus datos personales y también a conocer al aviso de privacidad, mediante el

cual se dio inicio al tratamiento de los datos personales.



Art. 46
LPDPPSOEJ

Derecho de Rectificación

El o la titular tendrá derecho a solicitar por sí o por su representante, la rectificación o corrección de sus datos personales, cuando resulten inexactos, incompletos, erróneos o no se encuentren actualizados.

Si este derecho se observa a la luz del principio de calidad, por el cual los datos personales deben ser ciertos, este derecho permite velar por que la información disponible en las bases de datos sea exacta y completa.

La rectificación busca controlar la calidad de los datos personales, en aras de enmendar errores en las bases de datos, y permite cumplir de manera adecuada el fin o finalidades del tratamiento de los datos personales.



Art. 46
LPDPPSOEJ

Derecho de Cancelación

El o la titular tendrá derecho a solicitar la cancelación o eliminación de sus datos personales de los archivos, registros,

expedientes y sistemas del responsable, a fin de que ya no estén en su posesión, ya que el tratamiento no se encuentra ajustado a lo establecido en Ley.

Como resultado del ejercicio de este derecho el responsable deberá bloquear los datos personales y posteriormente suprimirlos.



Art. 46
LPDPPSOEJ

Derecho de Oposición

El o la titular podrá oponerse al tratamiento de sus datos personales o exigir que cese el mismo, cuando no se ajuste a las finalidades o a lo dispuesto por la Ley o aun siendo lícito, cause un daño o perjuicio al titular.

El titular solicitará que sus datos dejen de ser tratados, en caso de que no se le haya requerido su consentimiento, lo cual implica la ilicitud del tratamiento.

Cuando el tratamiento sea automatizado, y éste produzca efectos no deseados y/o afecte de manera significativa sus intereses, derecho o libertades.



**Arts. 47-51
LPDPSOEJ**

Medios para presentar una solicitud de derechos ARCO

Requisitos para el ejercicio de los derechos ARCO

- Nombre del Titular
- Documentos que acrediten la identidad del Titular
- De ser posible, área del responsable que trata los DP
- Domicilio o medio para recibir notificaciones
- Descripción clara y precisa de los DP de los que se busca ejercer alguno de los derechos ARCO
- Descripción del derecho ARCO que se pretende ejercer
- Cualquier elemento que facilite la localización de los datos personales en cuestión

La solicitud para ejercer estos derechos se presenta ante las Unidades de Transparencia de los sujetos obligados a quienes corresponda el tratamiento de los datos personales que se pretende controlar o que el titular considere competente, a través de cualquiera de los siguientes medios:

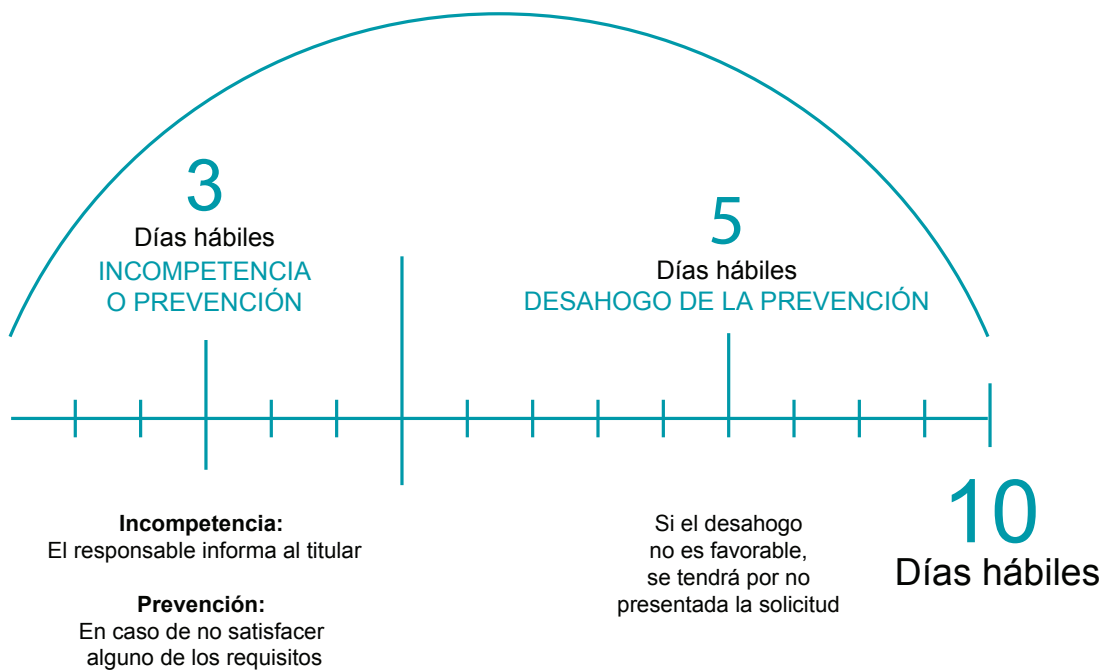
- Escrito libre
- Formatos
- Medios electrónicos
- O cualquier medio que sea facilitado por el Instituto para este fin



**Arts. 53-62
LPDPPSOEJ**

Plazos de respuesta Para el ejercicio de los derechos ARCO

El plazo de 10 días puede ser ampliado por un plazo de cinco días, siempre y cuando se justifique esta situación. En caso de resultar procedente, el responsable tiene un plazo de 5 días para hacer efectiva la solicitud, a partir de la emisión de la resolución.





**Arts. 88-89
LPDPPSOEJ**

Responsables en materia de protección de datos personales en posesión de sujetos obligados

Unidad de transparencia

Son las unidades administrativas receptoras de las solicitudes de ejercicio de derechos ARCO, dan trámite y atienden las solicitudes; son el vínculo directo entre los sujetos obligados y las personas. Dependerá del Titular del sujeto obligado.

Algunas atribuciones de la Unidad de Transparencia son:

- Auxiliar y orientar al titular con relación al ejercicio de los derechos ARCO y la protección de datos personales.
- Gestionar las solicitudes para el ejercicio de los derechos ARCO.
- Proponer al Comité de Transparencia los procedimientos que aseguren y fortalezcan la gestión de las solicitudes de los derechos ARCO.
- Asesorar a las áreas del sujeto obligado en materia de protección de datos personales.
- Podrá dar aviso al superior jerárquico en caso de que algún área se niegue a colaborar.



**Art. 87
LPDPPSOEJ**

Comité de transparencia

Órgano Colegiado al interior de cada sujeto obligado integrado por número impar de personas servidoras públicas, que no dependerán jerárquicamente entre sí.

¿Qué funciones tiene?

- Instituir procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO.
- Confirmar, modificar o revocar la declaración de la inexistencia de los datos personales.
- Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.



Art. 90
LPDPPSOEJ

El ITEI y la protección de datos personales

Es el organismo autónomo del Estado de Jalisco, especializado, independiente, imparcial y colegiado. Facultado para dirigir y vigilar el ejercicio de los Derechos de Acceso a la Información y de **Protección de Datos Personales**.

El Pleno del ITEI se encuentra conformado por 2 comisionados ciudadanos o comisionadas ciudadanas, y un comisionado presidente.

Atribuciones del ITEI en materia de datos personales:

- Difundir el derecho de protección de datos personales.
- Resolver los recursos de revisión en materia de datos personales.
- Llevar a cabo acciones y actividades que promuevan el conocimiento del derecho a la protección de datos personales
- Coordinarse y promover el derecho a la protección de datos personales entre los responsables de manera permanente



Art. 99
LPDPPSOEJ

Medios de defensa en materia de protección de datos personales

Recurso de revisión

Es un medio de defensa que puede hacer valer quien ejerza alguno de los Derechos ARCO, en contra de las respuestas u omisiones de los sujetos obligados. Se podrá interponer dentro de los 15 días siguientes contados a partir de la notificación de la respuesta a la solicitud de derechos ARCO o de que transcurrió el plazo para dar una respuesta.

El recurso de revisión procederá, entre otras causas, por:

- La inexistencia de los datos personales.
- La declaración de incompetencia por el sujeto obligado.
- La entrega de datos personales incompletos.
- La entrega de datos personales que no correspondan con lo solicitado.
- La negativa al acceso, rectificación, cancelación u oposición de datos personales.
- La falta de respuesta a una solicitud ARCO, dentro de los plazos establecidos en la ley.
- Los costos de reproducción o tiempos de entrega de los datos personales.
- La falta de trámite a una solicitud para el ejercicio de los derechos ARCO.



**Arts. 99-101
LPDPPSOEJ**



**Arts. 82-105
LPDPPSOEJ**

Plazos

DÍA 1 Presentación del Recurso de revisión (RR)

El recurso de revisión podrá presentarse ante la Unidad de Transparencia del sujeto obligado que dio u omitió dar respuesta a la solicitud o ante el ITEI, mediante los medios que dispone la Ley. Para lo cual, tendrá que acreditar su identidad y cumplir con los siguientes requisitos:

Sujeto obligado a quien se presentó la solicitud de derechos ARCO
Nombre del o la titular de los datos personales (re- currente) o su representante.
Fecha de notificación de respuesta a la solicitud de derechos ARCO
Acto o resolución que se recurre; así como la moti- vación de la inconformidad.
Documentos que acrediten la identidad del o la ti- tular.

DÍA 5 Acuerdo del ITEI

Dentro de los tres días siguientes el ITEI tendrá que emitir un acuerdo por el cual:

- **Admite** a trámite el recurso de revisión.
- **Previene**, al ahora recurrente, en caso de que no sea claro el texto o falte alguno de los requisitos y éste no pueda ser subsanado por el ITEI.
- La prevención tiene el efecto de interrumpir el plazo que tiene el ITEI para resolver el recurso.
- **Desecha**, en caso de presentarlo fuera del plazo establecido.

DÍA 10 Atención a la prevención

La prevención al recurrente realice el organismo garante, tendrá que atenderse en un plazo no mayor a cinco días.

Falta de respuesta

El ITEI dará al sujeto obligado un plazo no mayor de 5 días para que alegue lo que su derecho convenga por la falta de respuesta, y una vez recibida la contestación dará un plazo de tres días para que atienda la solicitud de derechos ARCO.



Arts. 107-110 LPDPPSOEJ

DÍA 7 Disposición del expediente y ofrecimiento de pruebas y alegatos

Una vez admitido el recurso e integrado el expediente se pondrá a disposición de las partes y en un plazo máximo de siete días podrán manifestar lo que consideren, o en su caso, manifestar la voluntad de conciliar.

CONCILIACIÓN

Podrá celebrarse:

- Presencialmente
- Medios electrónicos
- Cualquiera que esté autorizado por el Instituto

10 DÍAS Elaboración de proyecto

Una vez desahogadas las pruebas y alegatos, se declara el cierre de instrucción y en un plazo que no exceda 10 días el Comisionado o Comisionada a quien fue turnado en recurso elaborará un proyecto de resolución, el cual será presentado al Pleno, quien por mayoría adoptará una resolución en un plazo no mayor a 20 días.

DÍA 20: El plazo de 20 días puede ampliarse por 10 días más.

Facultad de atracción

El **INAI** cuenta con una **facultad de atracción**, mediante la cual puede conocer y resolver los recursos promovidos ante el ITEI, en casos de interés o trascendencia.

Esta facultad puede ejercerse de oficio o a petición de los organismos garantes, el ejercicio de esta facultad se encuentra regulada por los Lineamientos Generales para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ejerza la facultad de atracción.



**Arts. 110
LPDPSOEJ**

Sentidos de las resoluciones del ITEI:

CONFIRMAR	El ITEI confirma la respuesta del sujeto obligado
SOBRESEER	<p>Terminar con el procedimiento de manera anticipada, sin que necesariamente se estudie en fondo del asunto.</p> <p>Ocurre cuando:</p> <p>El recurrente se desiste, fallece, por la actualización de alguna causal de improcedencia o por quedar sin materia</p>
DESECHAR	<p>Por ser extemporáneo, cuando no se acredita debidamente la identidad, o por no haber atendido la prevención.</p>
MODIFICAR O REVOCAR	<p>Podrá ser modificada o revocada</p>
ORDENAR	<p>Se instruye al responsable para atender la solicitud ARCO, en caso de omisión.</p>
<p>Las resoluciones del Instituto son vinculantes, definitivas e inatacables.</p>	



**Arts. 110
LPDPSOEJ**

Recurso de inconformidad y amparo

Los particulares podrán impugnar las determinaciones o resoluciones del ITEI ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), a través de un recurso de inconformidad; o ante el Poder Judicial, mediante un amparo. Pero nunca se agotarán ambas vías al mismo tiempo.

La resolución del INAI será definitiva e inatacable para el organismo garante (ITEI) y el sujeto obligado. Sin embargo, el particular podrá impugnar, de nueva cuenta, las resoluciones del INAI ante el Poder Judicial de la Federación, mediante un AMPARO.



**Arts. 136-138
LPDPSOEJ**

Cumplimiento de las resoluciones

Los sujetos obligados a través, de la Unidad de Transparencia darán cumplimiento a las resoluciones del ITEI.

El sujeto obligado deberá informar al ITEI sobre el cumplimiento de la resolución El ITEI verificará de oficio la información, a más tardar al día siguiente de recibir el oficio de cumplimiento, y dará vista al recurrente.

Si el ITEI considera que el sujeto obligado da cumplimiento, se emitirá un Acuerdo de cumplimiento. En caso contrario el ITEI:

1. Emitirá un acuerdo de incumplimiento
2. Notificará al superior jerárquico del responsable de dar cumplimiento.
3. Determinará las medidas de apremio o sanciones.



**Arts. 139-146
LPDPPSOEJ**

Medidas de apremio y sanciones

El Instituto podrá imponer a la persona encargada de cumplir con la resolución, las siguientes medidas de apremio para asegurar el cumplimiento de sus determinaciones:

- Amonestación pública o
- Multa de ciento cincuenta hasta mil quinientas veces la unidad de medida vigente en el Estado de Jalisco.
- Arresto administrativo

Las multas nunca se pagan con recursos públicos, sino que las pagarán, en su caso, los servidores públicos.

Causales

Algunas de las causales son:

- Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;
- Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;
- Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
- Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;
- No recabar el consentimiento del o la titular, lo que constituye que el tratamiento sea ilícito, o no contar con el aviso de privacidad; o bien, tratar de manera dolosa o con engaños datos personales, y las demás disposiciones que resulten aplicables en la materia;



3.4.1 Evaluación formativa

Concluido el tercer módulo anotará sus ideas relacionadas con los siguientes tópicos, con el objetivo de reforzar conocimientos de los puntos más relevantes.

1. Mencione usted 3 principios y 3 deberes que debe cumplir el Responsable del tratamiento de datos personales

2. Indique los plazos de atención de las solicitudes de derecho ARCO

3. Señale usted los requisitos de una solicitud de derechos ARCO.

4. Mencione algunas causas de procedencia del Recurso de revisión

5. Señale tres requisitos del recurso de revisión

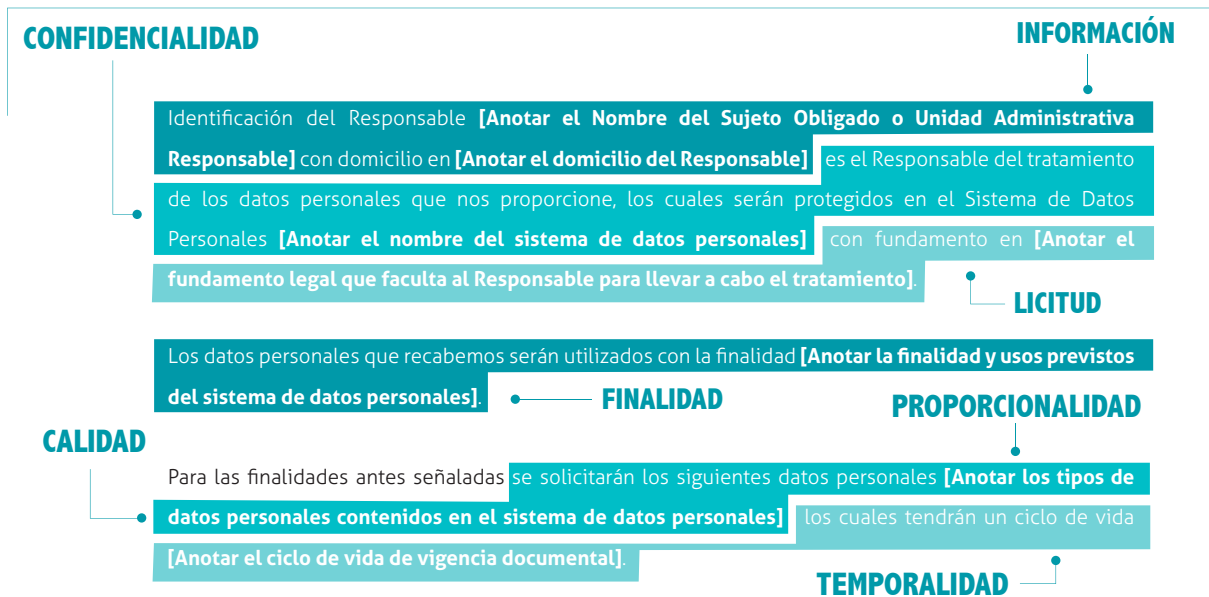
4. Anexos

Anexo 1. APLICACIÓN DE LOS PRINCIPIOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE JALISCO

ANATOMÍA DEL AVISO DE PRIVACIDAD

FORMATO DE AVISO DE PRIVACIDAD

TRANSPARENCIA/ INFORMACIÓN



Usted podrá ejercer sus derechos de acceso, rectificación, cancelación u oposición, de sus datos personales (derechos ARCO), así como la revocación del consentimiento directamente ante la Unidad de Transparencia de **[Anotar el Nombre del Sujeto Obligado]**, ubicada en **[Anotar el domicilio de la Unidad de Transparencia]** con número telefónico **[Anotar el número telefónico de la Unidad de Transparencia]**, o bien, a través de la Plataforma Nacional de Transparencia (<http://www.plataformadetransparencia.org.mx/>), o en el correo electrónico **[Anotar el correo electrónico de la Unidad de Transparencia del Sujeto Obligado]**.

Si desea conocer el procedimiento para el ejercicio de estos derechos puede acudir a la Unidad de Transparencia, enviar un correo electrónico a la dirección antes señalada o comunicarse al TELEFONO DEL ITEI

Firma del titular de los datos personales

CONSENTIMIENTO

5. Bibliografía y referencias

Piñar, Mañas, José Luis; y Ornelas Nuñez, Lina, La protección de Datos Personales en México, Tirant Lo Blanch, México, 2013.

Tenorio Cueto, Guillermo (Coord.), Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares, Porrúa, México, 2011.

García, Ricci, Diego, Para entender el Derecho a la Privacidad, Nostra Ediciones, México, 2017.

Garzón, Valdez, Ernesto, Lo íntimo, lo privado y lo público, Cuadernos de transparencia número 6, INAI, México, 2015. Disponible en <http://inicio.ifai.org.mx/PublicacionesComiteEditorial/Cuadernillo%2006%20B.pdf>

Escalante, Gonzalbo, Fernando, El derecho a la privacidad, Cuadernos de transparencia número 2, INAI, México, 2015. Disponible en <http://inicio.ifai.org.mx/PublicacionesComiteEditorial/Cuadernillo%2002%20B.pdf>

Legislación local

Constitución política del Estado de Jalisco. Congreso del Estado de Jalisco. Periódico Oficial del Estado de Jalisco, 01 de agosto de 1917.

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios. Periódico oficial del Estado de Jalisco, 26 de julio del 2016.

Legislación nacional

Constitución Política De Los Estados Unidos Mexicanos (Artículos 1, 6, 16 y 73, fracción XIXI-O), disponible en <http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum.htm>

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO), 26 de enero de 2017, disponible en <http://www.diputados.gob.mx/LeyesBiblio/ref/lgpdppso.htm>

Ley de Protección de Datos Personales en Posesión de Particulares, 5 de julio 2010, disponible en <http://www.diputados.gob.mx/LeyesBiblio/ref/lfpdppp.htm>

Reglamento de la Ley de Protección de datos Personales en Posesión de Particulares, 21 de diciem-

bre de 2011, disponible en http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

Ley General de Salud (Artículo Transitorio Tercero), disponible http://www.diputados.gob.mx/LeyesBiblio/pdf/142_241218.pdf

Norma Oficial Mexicana NOM-024-SSA3-2010, Que establece los objetivos funcionales y funcionalidades que deberán observar los productos de Sistemas de Expediente Clínico Electrónico para garantizar la interoperabilidad, procesamiento, interpretación, confidencialidad, seguridad y uso de estándares y catálogos de la información de los registros electrónicos en salud, 8 de septiembre de 2010, disponible en. http://www.dgis.salud.gob.mx/descargas/pdf/NOM-024-SSA3-2010_SistemasECE.pdf

Norma Oficial Mexicana NOM-004-SSA3-2012, Del expediente clínico, 30 de noviembre de 2012, disponible en <http://www.dgis.salud.gob.mx/descargas/pdf/NOM-024-SSA3-2012.pdf>

Ley General de Transparencia y Acceso a la Información Pública, 4 de mayo de 2015, disponible en <http://www.diputados.gob.mx/LeyesBiblio/ref/lgtaip.htm>

Recomendaciones en materia de seguridad de datos personales, 30 de octubre de 2013, disponible en https://www.dof.gob.mx/nota_detalle_popup.php?codigo=5320179

Lineamientos Generales de Protección de Datos Personales para el Sector Público., 28 de enero de 2018, disponible en http://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018

Legislación internacional

Marco de privacidad del foro de Cooperación Económica Asia- Pacífico (APEC) [2005] disponible en <https://archivos.juridicas.unam.mx/www/bjv/libros/12/5669/19.pdf>

Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales (Recomendación del Consejo de la OCDE) disponible en <http://inicio.ifai.org.mx/DocumentosdelInteres/OCDE-Directrices-sobre-proteccion-de-privacidad-Trad.pdf>

Convenio No 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de la personas con respecto al tratamiento automatizado de datos de carácter personal disponible en <http://www.oas.org/es/sla/ddi/docs/U12%20convenio%20n%20108.pdf>

Protocolo adicional del Convenio No 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de la personas con respecto al tratamiento automatizado de datos de carácter per-

sonal, Estrasburgo, 8 de noviembre 2008 disponible en https://www.dof.gob.mx/nota_detalle.php?codigo=5539474&fecha=28/09/2018

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32002L0058&from=ES>

Estándares Internacionales sobre Protección de Datos Personales y Privacidad Resolución de Madrid disponible en https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf

Resolución 45/95, 14 de diciembre de 1990, Principios Rectores para la Reglamentación de los Ficheros Computadorizados de Datos Personales disponible en <http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf>

Estándares de Protección de Datos Personales para los Estados Iberoamericanos, disponible en <https://www.redipd.org/es/documentos/estandares-iberoamericanos>



INSTITUTO DE TRANSPARENCIA, INFORMACIÓN PÚBLICA
Y PROTECCIÓN DE DATOS PERSONALES
DEL ESTADO DE JALISCO



CESIP

Centro de Estudios Superiores de
la Información Pública y
Protección de Datos Personales

MANUAL DE PARTICIPANTE:
**CURSO: INTRODUCCIÓN A LA PROTECCIÓN DE DATOS PERSONALES
EN POSESIÓN DE SUJETOS OBLIGADO DEL ESTADO DE JALISCO**