

GUÍA PARA EL TRATAMIENTO DE DATOS PERSONALES CONTENIDOS EN EXPEDIENTES DE PERSONAL DE LOS RESPONSABLES



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

TABLA DE CONTENIDO

Glosario	2
Introducción	5
Aplicación de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.....	6
Principios	6
Recomendaciones para cumplir con cada principio	7
Principio de Licitud	7
Principio de Finalidad	12
Principio de Proporcionalidad	15
Principio de Información	17
Principio de Lealtad.....	22
Principio de Consentimiento	23
Principio de Calidad	24
Principio de Responsabilidad	27
Material del Referencia	28

GLOSARIO

Áreas: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales;

Aviso de privacidad: Documento físico, electrónico o en cualquier formato generado por el responsable, que es puesto a disposición del titular con el objeto de informarle los propósitos principales del tratamiento al que serán sometidos sus datos personales;

Bases de Datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

Bloqueo: La identificación y conservación de los datos personales, una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual correspondiente. Durante dicho período los datos personales no podrán ser objeto de tratamiento y concluido éste se deberá proceder a la supresión en la base de datos, archivo, registro, expediente o sistema de información que corresponda;

Comité de Transparencia: Comité de Transparencia de cada sujeto obligado en los términos de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios y demás disposiciones aplicables;

Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos digitales, en recursos compartidos dinámicamente;

Consentimiento: Manifestación de la voluntad libre, específica e informada del titular que autoriza el tratamiento de sus datos personales;

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

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

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

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

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

Ley: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Jalisco y sus Municipios;

Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

Medidas compensatorias: Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance;

Medidas de seguridad: conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales;

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

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

- a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir fuera de las instalaciones de la organización; y
- d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

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

Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, con independencia de que se realice dentro o fuera del territorio mexicano;

Responsable: Los sujetos obligados señalados en el artículo 1, párrafo 5, de la presente Ley que determinarán los fines, medios y alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

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

Titular: Persona física a quien pertenecen los datos personales;

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

Tratamiento: De manera enunciativa más no limitativa 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; y

Unidad de Transparencia: Instancia que funge como vínculo entre el responsable y el titular, siendo la misma a la que se hace referencia en el artículo 31 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

INTRODUCCIÓN

El objetivo principal de esta Guía de Tratamiento, es acompañar a los Responsables para que cumplan con todas las obligaciones señaladas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios (LPDPPSOEJ), dentro del Sistema de Tratamiento de los Expedientes de Personal, pues dicho Sistema es el primer acercamiento que tienen los Responsables a los datos personales de los servidores públicos. Esta Guía es derivada de los procedimientos de verificación preventivos realizados a diversos sujetos obligados el 05 de septiembre del 2018, los cuales arrojaron un diagnóstico sobre el tratamiento y el nivel de cumplimiento promedio de los sujetos obligados en el Estado de Jalisco.

APLICACIÓN DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE JALISCO Y SUS MUNICIPIOS

Son sujetos obligados en el ámbito estatal y municipal, cualquier autoridad, entidad, órgano y organismo del Poder Ejecutivo, Legislativo y Judicial, ayuntamientos, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, que lleven a cabo el tratamiento de datos personales.

Los sindicatos y cualquier otra persona física o jurídica que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares, sin perjuicio de lo previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Jalisco y sus Municipios es aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia del lugar, la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

PRINCIPIOS

Con la entrada en vigor de la LPDPPSOEJ, el 26 de julio de 2017, se reconocen una serie de principios, deberes y derechos rectores de la protección de datos personales, de observancia obligatoria para los particulares y sujetos obligados del sector público que tratan datos personales, y que en su conjunto garantizan un adecuado manejo de los mismos, a favor de la privacidad y de la autodeterminación informativa de los titulares. De acuerdo con la citada ley, los principios rectores de la protección de datos personales son:



RECOMENDACIONES PARA CUMPLIR CON CADA PRINCIPIO

PRINCIPIO DE LICITUD

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Artículo 10. Principios — Licitud.

1. 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.

Primeramente, es importante identificar todos los datos personales que se recaban, sin pasar por alto ningún dato, como a continuación se ejemplifica:

- Nombre
- Edad
- Sexo
- Domicilio
- Número telefónico particular
- Número telefónico celular
- Clave Única de Registro de Población
- Clave del Registro Federal de Contribuyentes
- Clave de elector (Instituto Nacional de Electoral)
- Firma
- Estado Civil
- Fotografía
- Nacionalidad
- Correo electrónico

De cada uno de los datos personales que se recaban, se debe buscar el fundamento legal que otorga la atribución para recabarlos. Los fundamentos legales deben ser aplicables al sujeto obligado, señalando con precisión la Ley, el artículo, inciso, fracción y párrafo¹ correspondiente, como a continuación se ejemplifica:

Dato Personal	Fundamento Legal	Artículo
Nombre	Ley para los Servidores Públicos del Estado de Jalisco	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil, domicilio, clave única de registro de población y registro federal de contribuyentes;
Edad	Ley para los Servidores Públicos del Estado de Jalisco	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil, domicilio, clave única de registro de población y registro federal de contribuyentes;
Sexo	Ley para los Servidores Públicos del Estado de Jalisco	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil, domicilio, clave única de registro de población y registro federal de contribuyentes;
Domicilio	Ley para los Servidores Públicos del Estado de Jalisco	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil,

¹ Tesis 216534. VI. 2o. J/248. Tribunales Colegiados de Circuito. Octava Época. Gaceta del Semanario Judicial de la Federación. Núm. 64, Abril de 1993, Pág. 43

		domicilio, clave única de registro de población y registro federal de contribuyentes;
Constancia de no antecedentes penales	Condiciones Generales de Trabajo del ITEI	Artículo 13. Las personas que aspiren a laborar como servidores públicos del Instituto, deberán reunir los siguientes requisitos: III. Estar en pleno uso de sus derechos civiles;
Número telefónico celular		
Clave Única de Registro de Población	Ley para los Servidores Públicos del Estado de Jalisco	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil, domicilio, clave única de registro de población y registro federal de contribuyentes;
Clave del Registro Federal de Contribuyentes	Ley para los Servidores Públicos del Estado de Jalisco	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil, domicilio, clave única de registro de población y registro federal de contribuyentes;
Clave del Instituto Nacional de Elector		
Número de Seguro Social	Ley para los Servidores Públicos del Estado de Jalisco	Artículo 56.- Son obligaciones de las Entidades Públicas, en las relaciones laborales con sus servidores: XII. Proporcionar servicios médicos, quirúrgicos, hospitalarios, farmacéuticos y asistenciales a los servidores públicos o, en su

		caso, afiliarlos a través de convenios de incorporación, al Instituto Mexicano del Seguro Social, o a alguna institución federal, estatal u organismo público descentralizado, que sea instrumento básico de la seguridad social;
Número de Afiliado al IPEJAL	Ley para los Servidores Públicos del Estado de Jalisco	Artículo 56.- Son obligaciones de las Entidades Públicas, en las relaciones laborales con sus servidores: XIII. Otorgar las jubilaciones conforme lo dispone la Ley del Instituto de Pensiones del Estado de Jalisco;
Firma	Ley para los Servidores Públicos del Estado de Jalisco	Artículo 56.- Son obligaciones de las Entidades Públicas, en las relaciones laborales con sus servidores: XIV. Entregar al servidor público el duplicado de los nombramientos y movimientos de personal que sus criba, para lo cual el empleado firmará la constancia de entrega, misma que se adjuntará a su expediente;
Estado Civil	Ley para los Servidores Públicos del Estado de Jalisco	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil, domicilio, clave única de registro de población y registro federal de contribuyentes;
Fotografía	Manual de Procesos del Instituto de Transparencia, Información Pública y	11) Administración y desarrollo de personal Este proceso integra las

	Protección de Datos Personales del Estado de Jalisco.	acciones de desarrollo del personal del ITEI, además de la administración de sus recursos humanos. Se identifican los siguientes subprocesos y procedimientos: 11.3 Contratación del personal 11.3.1 Recepción de la documentación solicitada tal como se describe: - Dos fotografías tamaño credencial
Nacionalidad	Ley para los Servidores Públicos del Estado de Jalisco	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil, domicilio, clave única de registro de población y registro federal de contribuyentes;
Correo Electrónico		

Una vez que se identifiquen los datos personales recabados y los fundamentos legales de cada uno, todos los datos personales que no cuentan con fundamento legal para recabarlos, deben de suprimirse y dejar de recabarlos. Por ejemplo, en la tabla anterior, los datos que no cuentan con fundamento legal para ser recabados son: correo electrónico, número telefónico particular y clave del Instituto Electoral, en consecuencia, se debe cesar su tratamiento.

De esta manera, todos los datos personales que se recaben en el sujeto obligado se encuentran respaldados por un fundamento legal.

PRINCIPIO DE FINALIDAD

Artículo 11. Principios — Finalidad.

1. Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, explícitas, lícitas y legítimas y deberá sujetarse a los principios contenidos en el presente capítulo, relacionadas con las facultades y atribuciones que la normatividad aplicable les confiera.

2. Se entenderá que las finalidades son:

I. Concretas: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que sea posible la existencia de finalidades genéricas que puedan generar confusión en el titular;

II. Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad, y

III. Lícitas y legítimas: cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones expresas del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional aplicable.

Después de identificar nuestro inventario de datos personales, debemos describir las finalidades para las que se recaban cada uno de los datos, estas finalidades deben de ser claras, específicas y explícitas, evitando usar palabras o frases genéricas como “otras finalidades”, “diversos trámites”, “etcétera”, “posibles situaciones”, “trámites distintos”, “entre otros” para que las mismas cumplan con la característica de ser concretas y explícitas.

Para que las finalidades sean lícitas y legítimas, deben ser comparadas con el fundamento legal, cuidando que exista congruencia entre lo señalado por el fundamento legal y la finalidad expresa, tal y como se puede observar en el siguiente ejemplo:

Dato Personal	Fundamento Legal	Finalidad concreta, lícita y explícita
Nombre	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil, domicilio, clave única de registro de población y registro federal de contribuyentes;	Se recabará para expedir el respectivo nombramiento del servidor público.
Edad	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil, domicilio, clave	Se recabará para expedir el respectivo nombramiento del servidor público.

	única de registro de población y registro federal de contribuyentes;	
Sexo	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil, domicilio, clave única de registro de población y registro federal de contribuyentes;	Se recabará para expedir el respectivo nombramiento del servidor público.
Domicilio	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil, domicilio, clave única de registro de población y registro federal de contribuyentes;	Se recabará para expedir el respectivo nombramiento del servidor público.
Constancia de no antecedentes penales	Artículo 13. Las personas que aspiren a laborar como servidores públicos del Instituto, deberán reunir los siguientes requisitos: III. Estar en pleno uso de sus derechos civiles;	Se recabará para comprobar que el aspirante al puesto cumpla con todos los requisitos para laborar en el Responsable señalados en las Condiciones Generales de Trabajo.
Clave Única de Registro de Población	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil, domicilio, clave única de registro de población y registro federal de contribuyentes;	Se recabará para expedir el respectivo nombramiento del servidor público.
Clave del Registro Federal de Contribuyentes	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil, domicilio, clave única de registro de población y registro federal de contribuyentes;	Se recabará para expedir el respectivo nombramiento del servidor público.
Número de Seguro Social	Artículo 56.- Son obligaciones de las Entidades Públicas, en las relaciones laborales con sus servidores: XII. Proporcionar servicios médicos, quirúrgicos, hospitalarios, farmacéuticos y	Se recabará para otorgarle al servidor público su derecho a contar con seguro social.

	asistenciales a los servidores públicos o, en su caso, afiliarlos a través de convenios de incorporación, al Instituto Mexicano del Seguro Social, o a alguna institución federal, estatal u organismo público descentralizado, que sea instrumento básico de la seguridad social;	
Número de Afiliado al IPEJAL	Artículo 56.- Son obligaciones de las Entidades Públicas, en las relaciones laborales con sus servidores: XIII. Otorgar las jubilaciones conforme lo dispone la Ley del Instituto de Pensiones del Estado de Jalisco;	Se recabará para otorgar al servidor público su derecho a pensión por jubilación.
Firma	Artículo 56.- Son obligaciones de las Entidades Públicas, en las relaciones laborales con sus servidores: XIV. Entregar al servidor público el duplicado de los nombramientos y movimientos de personal que sus criba, para lo cual el empleado firmará la constancia de entrega, misma que se adjuntará a su expediente;	Se recabará para entregar el nombramiento al servidor público correspondiente y comprobar mediante la firma que fue recibido.
Estado Civil	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil, domicilio, clave única de registro de población y registro federal de contribuyentes;	Se recabará para expedir el respectivo nombramiento del servidor público.
Fotografía	11) Administración y desarrollo de personal Este proceso integra las acciones de desarrollo del personal del ITEI, además de la administración de sus recursos humanos. Se identifican los siguientes subprocesos y procedimientos: 11.3 Contratación del personal 11.3.1 Recepción de la	Se recabará para generar la credencial de identificación que se utilizará dentro de las instalaciones del Responsable como medida de seguridad administrativa, así como para colocar la fotografía en el expediente laboral del servidor para su pronta identificación.

	documentación solicitada tal como se describe: - Dos fotografías tamaño credencial	
Nacionalidad	Artículo 17.- Los nombramientos deberán contener: I. Nombre, nacionalidad, edad, sexo, estado civil, domicilio, clave única de registro de población y registro federal de contribuyentes;	Se recabará para expedir el respectivo nombramiento del servidor público.

PRINCIPIO DE PROPORCIONALIDAD

Artículo 18. Principios — Criterio de minimización.

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

Una vez que tenemos identificados los datos personales que se recaban, los fundamentos legales para recabarlos y las finalidades, debemos aplicar el criterio de minimización tomando en cuenta las finalidades que hemos establecido anteriormente, para eliminar aquellos datos personales que no tienen relevancia en las finalidades señaladas.

Dato Personal	Acta de nacimiento	Credencial para votar	Comprobante de domicilio	Cédula de la CURP
Nombre	✓	✓	✓	✓
Domicilio	✗	✓	✓	✗
Edad	✓	✓	✗	✗
Nacionalidad	✓	✓	✗	✗
CURP	✗	✓	✗	✓

Por otro lado, debemos de reducir el número de documentos mediante los cuales se recaban los datos personales, dando prioridad a los que contengan menor número de datos personales que no son necesarios para el sistema de tratamiento. Por ejemplo, si se solicita el acta de nacimiento y la credencial para votar, debemos hacer una comparación de los datos personales que contienen:

Acta de Nacimiento	Credencial para votar
1. Nombre 2. Fecha de nacimiento 3. Lugar de Nacimiento 4. Sexo 5. Nombre del padre 6. Edad del padre 7. Nacionalidad del padre 8. Nombre de la madre 9. Edad de la madre 10. Nacionalidad de la madre 11. Nombre del abuelo paterno 12. Nacionalidad del abuelo paterno 13. Nombre de la abuela paterna 14. Nacionalidad de la abuela paterna 15. Nombre de la abuela materna 16. Nacionalidad de la abuela materna 17. Nombre del abuelo materno 18. Nacionalidad del abuelo materno 19. Nombre de testigo 20. Edad del Testigo 21. Nacionalidad del Testigo 22. Nombre de testigo 23. Edad del Testigo 24. Nacionalidad del Testigo	1. Nombre 2. Nacionalidad 3. Domicilio 4. Edad 5. CURP 6. Sexo 7. Clave de elector 8. Firma 9. Huella digital dedo índice

Podemos observar que el número de datos personales que contiene el acta de nacimiento es mucho mayor que los contenidos en la credencial para votar, por lo que debemos ponderar los datos que necesitamos recabar y cuales documentos los contienen:

Dato Personal	Acta de Nacimiento	Credencial para votar
Nombre	✓	✓
Edad	✓	✓
Nacionalidad	✓	✓
Domicilio	✗	✓
CURP	✗	✓

De dicha ponderación, tenemos que el documento con mayor número de datos personales relevantes para las finalidades del tratamiento que le daremos, es la credencial para votar, en

cambio el acta de nacimiento contiene menor número de datos relevantes para el tratamiento sin embargo contiene mayor número de datos personales innecesarios para el sistema de tratamiento, en consecuencia, se debe de priorizar la credencial para votar y dejar de solicitar el acta de nacimiento.

PRINCIPIO DE INFORMACIÓN

El principio de información se cumple a través del aviso de privacidad, ya que es el medio mediante el cual se da a conocer a los titulares el tratamiento que se le dará a sus datos personales, es por ello que el aviso de privacidad debe estar en todo momento a disposición de los titulares y debe ser mostrado antes de recabar los datos.

Artículo 20. Principios —Características del aviso de privacidad.

1. El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento. En el aviso de privacidad queda prohibido:

- I. Usar frases inexactas, ambiguas o vagas;
- II. Incluir textos o formatos que induzcan al titular a elegir una opción en específico;
- III. Marcar previamente casillas, en caso de que éstas se incluyan para que el titular otorgue su consentimiento; y
- IV. Remitir a textos o documentos que no estén disponibles para el titular.

Es importante señalar que el aviso de privacidad debe utilizar un lenguaje sencillo y muy claro, para que cualquier persona comprenda la forma en que se utilizarán sus datos. El principal objetivo del aviso de privacidad es que los titulares comprendan bajo qué condiciones estarán sus datos en posesión de sujetos obligados y para qué serán utilizados, por ello las frases vagas o ambiguas deben ser evitadas, algunos ejemplos de las frases que no deben utilizarse son:

- “Diversos procedimientos”.
- “Otros fines”.
- “Distintas funciones”.
- “Situaciones que puedan presentarse”.
- “Etcétera”.
- “Lo que en su caso corresponda”.

- “U otros”.
- “Entre otros”.
- “Distintos procesos/situaciones”.

La información dada al titular no debe inducirlo a tomar una decisión en específico, es decir, obligar al titular a tomar cierta postura o a otorgar su consentimiento, lo que va estrechamente ligado a no colocar casillas para otorgar el consentimiento que se encuentren ya marcadas. El aviso de privacidad no debe remitir a documentos que no estén disponibles para que el titular los revise en el momento, como podrían ser manuales, reglamentos, criterios entre otros. En resumen, el aviso de privacidad debe de darle al titular la libertad de auto determinar si entrega o no sus datos.

Artículo 24. Principios — Información, aviso de privacidad integral.

1. El aviso de privacidad integral, además de lo dispuesto en la fracción V del artículo anterior, deberá contener al menos, la siguiente información:

I. El domicilio del responsable;

II. Los datos personales que serán sometidos a tratamiento, identificando aquellos que son sensibles;

III. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;

IV. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieren el consentimiento del titular;

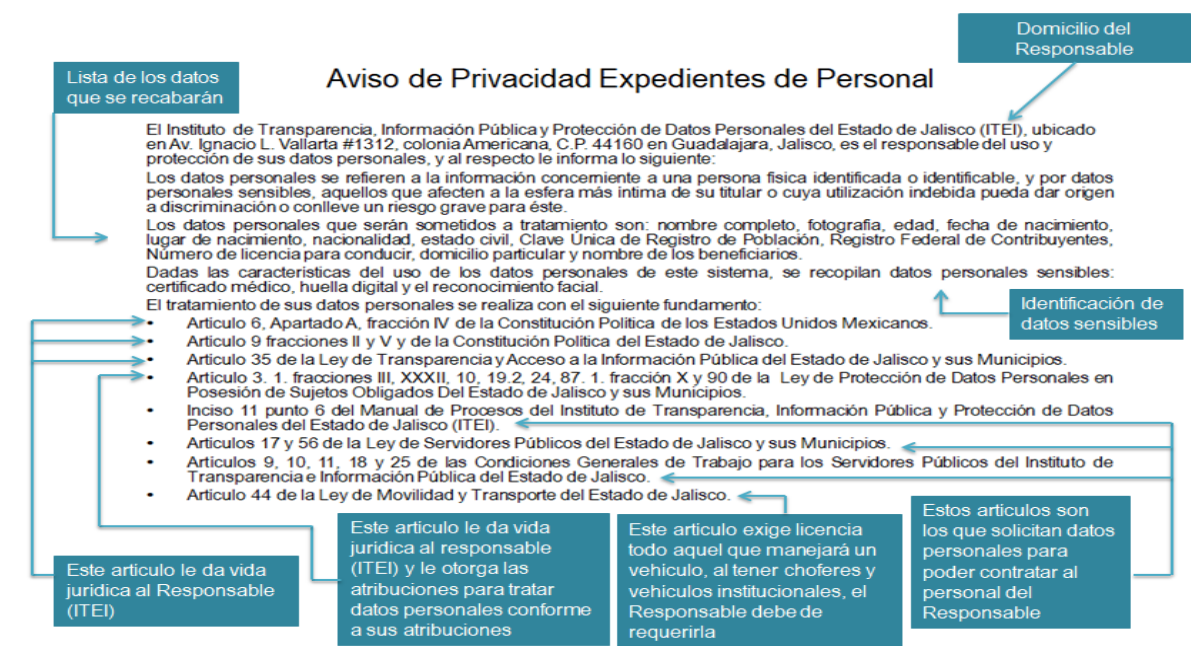
V. La información sobre el uso de mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que permita recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en su caso;

VI. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;

VII. El domicilio de la Unidad de Transparencia; y

VIII. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

Como buena práctica y para facilitar el cumplimiento de este principio, se recomienda realizar un aviso de privacidad focalizado en el Sistema de Tratamiento de Expedientes de Personal, el artículo anterior que señala el contenido del aviso de privacidad servirá como guía para redactarlo, como a continuación se ejemplifica:



Finalidades concretas y específicas

Los datos personales que usted proporcione al ITEI, serán única y exclusivamente utilizados para llevar a cabo los objetivos y atribuciones de este Instituto y los utilizaremos para las siguientes finalidades: Generar el expediente del personal, para el cumplimiento de las disposiciones administrativas como controles de acceso, contraseñas y medidas de seguridad, identificación y autenticación como servidor público, difusión de información pública de oficio, generar comprobantes de pago, cumplimiento de disposiciones fiscales y enteros de impuestos retenidos, emisión de constancias laborales, administrativas y de identificación; relativas al empleo, cargo o comisión, tales como el cumplimiento de los requisitos legales para la contratación y el pago de sueldos, salarios y prestaciones, historia laboral de los servidores públicos, cumplimiento de requisitos fiscales, administrativos y presupuestarios, altas, bajas y enteros en materias de seguridad social, aportaciones al Instituto de Pensiones del Estado, de identificación y localización del servidor público para fines laborales, administrativos y jurídicos, entradas y salidas del personal.

Asimismo, con el ingreso a nuestras instalaciones, podrá ser videograbado por nuestras cámaras de seguridad.

Cuando se realicen transferencias de datos personales se informará lo siguiente: Los datos personales consistentes en nombre, clave del Registro Federal de Contribuyentes, correo electrónico personal y pagos relacionados con sueldos, salarios y prestaciones serán transmitidos de manera quincenal o, en su caso, en los periodos en que se genere la obligación legal del pago, ante un proveedor de certificación de comprobantes fiscales digitales, así como al Servicio de Administración Tributaria, que lo concentrará en su buzón fiscal.

Se le informa que no se consideran transferencias las remisiones, ni la comunicación de datos entre áreas o unidades administrativas adscritas al mismo sujeto obligado en el ejercicio de sus atribuciones. No obstante, se hace de su conocimiento que los datos personales proporcionados de manera interna también serán utilizados para efectos de control interno, auditoría, fiscalización y, eventualmente, fincamiento de responsabilidades y atención de asuntos contenciosos, administrativos, judiciales y/o laborales, así como aquellos que deriven de la relación laboral-administrativa entre el servidor público y el Instituto.

Uso de mecanismos remotos para recabar datos personales

Información sobre las transferencias

Ejercicio de los derechos ARCO

Domicilio de la Unidad de Transparencia

Resulta importante que usted considere que, al brindar su consentimiento para la transmisión de los datos personales a las entidades a las que se hizo referencia, dicha información será tratada en un sistema de datos personales diverso al cual hace referencia el presente aviso de privacidad, por lo que se le sugiere consultar el aviso de privacidad que corresponda al sistema de datos personales en posesión del destinatario.

Usted puede solicitar ante el ITEI, en cualquier tiempo, su Acceso, Rectificación, Cancelación, Oposición o Revocación del consentimiento, mediante la presentación de solicitud de ejercicio de derechos ARCO ante la Unidad de Transparencia del ITEI, en Av. Ignacio L. Vallarta 1312, Colonia Americana, en Guadalajara Jalisco.

Cualquier cambio al presente aviso de privacidad se hará del conocimiento de los titulares de la información confidencial, a través de la página de internet de este sujeto obligado, la cual es: www.itei.org.mx

Forma de aviso sobre cambios

Artículo 19. Principios — Información.

1. El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.
2. El aviso de privacidad tendrá por objeto informar al titular sobre los alcances y condiciones generales del tratamiento, a fin de que esté en posibilidad de tomar decisiones informadas sobre el uso de sus datos personales y, en consecuencia, mantener el control y disposición sobre ellos.
3. El aviso de privacidad deberá ser difundido por los medios electrónicos y físicos con que se cuente, tales como medios impresos, sonoros, digitales, visuales o cualquier otra tecnología; con una redacción y estructura clara y sencilla, para cumplir con el propósito de informar.
4. Cuando resulte imposible dar a conocer al titular el aviso de privacidad de manera directa o ello exija esfuerzos desproporcionados, el responsable podrá instrumentar medidas compensatorias de comunicación masiva de acuerdo con los criterios que para tal efecto emita el Sistema Nacional.
5. El aviso de privacidad se redactará conforme a lo dispuesto en la Ley General.
6. En el caso de personas indígenas, el responsable hará los ajustes razonables pertinentes para dar a conocer el aviso de privacidad en su lengua de origen, con el objetivo de que el consentimiento sea considerado libre. Lo mismo aplicará para personas que comprendan el sistema braille y análogos.

El objetivo principal del aviso de privacidad es dar a conocer al titular el tratamiento que se le dará a sus datos personales recabados, por lo que es importante que el mismo se encuentre al alcance, ya sea por medio de la página web, pantallas, impreso, colocado en una pared, o cualquiera que permita a los titulares leerlo antes de entregar sus datos personales.

En razón de lo anterior, el responsable hará los ajustes razonables para dar a conocer el aviso a personas discapacitadas, como pueden ser:

Discapacidad	Ajuste
Visual	Traducirlo al sistema braille o leerlo en voz alta al titular.
Sonora	Darle a leer el aviso impreso o hacerlo de su conocimiento mediante lenguaje de señas.

Es indispensable que el Responsable tenga identificados los ajustes para dar a conocer su aviso de privacidad en cualquier circunstancia especial, para que en caso de que se presente la ocasión el Responsable pueda cumplir este principio sin contratiempos.

Ahora bien, dada la composición multicultural de nuestro país, el Responsable debe implementar los ajustes razonables para dar a conocer su aviso de privacidad a personas indígenas, lo cual se puede llevar a cabo mediante el padrón de intérpretes del micrositio “Transparencia al Alcance de Todos” de la página oficial del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco: <http://micrositios.itei.org.mx/alalcancedetodos/pci-modulo-2/>

En el mismo se podrán encontrar a intérpretes y traductores de distintas lenguas indígenas para solicitar su apoyo.

PRINCIPIO DE LEALTAD

Artículo 12. Principios — Lealtad.

1. El responsable no deberá obtener y tratar datos personales a través de medios engañosos o fraudulentos; deberá privilegiar la protección de los intereses del titular y la expectativa razonable de privacidad.
2. Se estará en presencia de un tratamiento engañoso o fraudulento o cuando:
 - I. Medie dolo, mala fe o negligencia en el tratamiento de datos personales que lleve a cabo;
 - II. Realice un tratamiento de datos personales que dé lugar a una discriminación injusta o arbitraria contra el titular, o
 - III. Vulnere la expectativa razonable de protección de datos personales.

El fundamento legal y las finalidades señaladas en el aviso de privacidad deben de ser congruentes con el tratamiento real que se le da a los datos personales, además el aviso de privacidad debe de señalar los datos personales sensibles a los que se les dará tratamiento, pues el titular debe de encontrarse informado sobre ello para no vulnerar la expectativa razonable de privacidad.

PRINCIPIO DE CONSENTIMIENTO

Artículo 14. Principios — Tipos de Consentimiento.

1. El consentimiento podrá manifestarse de forma expresa o tácita. El consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología. En el entorno digital, podrá utilizarse la firma electrónica o cualquier mecanismo o procedimiento equivalente que permita identificar fehacientemente al titular y, a su vez, recabar su consentimiento de tal manera que se acredite la obtención del mismo.
2. Para la obtención del consentimiento expreso, el responsable deberá facilitar al titular un medio sencillo y gratuito a través del cual pueda manifestar su voluntad.
3. Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando el aviso de privacidad es puesto a disposición y éste no manifiesta su voluntad en sentido contrario.
4. Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en esta Ley.

Al poner el aviso de privacidad en zonas de fácil acceso, a la vista o que se ponga a disposición de forma directa a los titulares, previa la entrega de sus datos personales, y se entenderá que el consentimiento es tácito, siempre y cuando el titular no manifieste lo contrario después de conocer el aviso. Sin embargo, cuando se tratan datos sensibles, es imprescindible que el titular otorgue su consentimiento expreso y por escrito, ya sea mediante el uso de formatos o cartas, siempre y cuando estos documentos sean claros sobre el tratamiento de datos sensibles y que no condicionen al titular para otorgar su consentimiento.

Artículo 13. Principios — Consentimiento.

1. Cuando no se actualicen algunas de las causales de excepción previstas en presente Ley, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:
 - I. Libre: sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular;
 - II. Específica: referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento; e
 - III. Informada: que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.
2. En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la Ley, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.

Para que el consentimiento se otorgue de forma libre, es importante que el aviso de privacidad entregado al titular se encuentre debidamente fundamentado y cumpliendo con todos los requisitos, pues de encontrarse incorrecto o incompleto, media error en el consentimiento.

Si las finalidades descritas en el aviso de privacidad, cumplen con lo establecido por el principio de finalidad, el consentimiento se otorga de forma específica. De igual forma, si el aviso de privacidad cumple con lo establecido por el principio de información, se entiende que el consentimiento se otorga de forma informada.

Por lo tanto, si se cumple con el principio de licitud, finalidad e información, reflejados en el aviso de privacidad que se le da a conocer a los titulares, previa a la recolección de los datos personales, el consentimiento se otorga de forma libre, específica e informada.

Si se recaban datos personales a través de terceros, por ejemplo datos de beneficiarios o de recomendaciones laborales, se debe implementar un mecanismo para recabar el consentimiento de los titulares y mostrarles el aviso de privacidad, pueden ser formatos específicos o que firmen el aviso de privacidad para otorgar su consentimiento.

PRINCIPIO DE CALIDAD

Artículo 16. Principios — Calidad.

1. El principio de calidad de los datos personales 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.
2. 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.
3. Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones aplicables, deberán ser suprimidos, previo bloqueo en su caso y una vez que concluya el plazo de conservación de los mismos.

Reducir al mínimo los datos personales que se recaban a través de terceros, beneficia al principio de calidad, pues evita que se obtengan datos personales que no se puedan mantener correctos ni actualizados. Si los datos personales se recaban directamente de los titulares, se presume que los mismos se mantienen correctos y actualizados, pero como buena práctica y para garantizar la

calidad de los datos personales recabados, al momento de recolectar los datos se hace del conocimiento del titular que en caso de que requiera actualizar sus datos se acerque al área correspondiente para que se lleven a cabo las gestiones adecuadas.

Artículo 17. Documentación de los procedimientos de conservación, bloqueo y supresión de los datos personales.

1. El responsable deberá establecer y documentar los procedimientos para la conservación, en su caso bloqueo y supresión de los datos personales en su posesión, en los cuales se incluyan los plazos de conservación de los mismos, conforme al artículo anterior.

2. En los procedimientos antes señalados el responsable deberá incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódica sobre la necesidad de su conservación.

Los datos personales deberán ser conservados, bloqueados y suprimidos, atendiendo al ciclo de vida de los datos personales, dicho procedimiento debe de documentarse y puede ser incluido en el documento de seguridad del Responsable.

Para este procedimiento, la Ley General de Archivos contempla un capítulo (artículo 60 al 63) en cuanto a la conservación de los archivos, por lo que puede servir de base para establecerlo en relación a los datos personales.

Ahora bien, el Responsable debe contemplar mecanismos de bloqueo de datos personales, para evitar que una vez que el tratamiento de los mismos ha llegado su fin, se tenga acceso no autorizado a los mismos o que sean utilizados ilícitamente.

Finalmente, se deben tener identificadas las técnicas de supresión y borrado seguro de los datos personales, que se adapten al tratamiento que le da el Responsable a los datos, algunos ejemplos de técnicas son las siguientes²:

Desmagnetización

La desmagnetización consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo.

Este método es válido para la destrucción de datos de los dispositivos magnéticos, como por ejemplo, los discos duros, disquetes, cintas magnéticas de *backup*, etc. Cada dispositivo, según su

² https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf

tamaño, forma y el tipo de soporte magnético del que se trate, necesita de una potencia específica para asegurar la completa polarización de todas las partículas.

Destrucción física

El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo para evitar la recuperación posterior de los datos que almacena. Existen diferentes tipos de técnicas y procedimientos para la destrucción de medios de almacenamiento: desintegración, pulverización, fusión e incineración: son métodos diseñados para destruir por completo los medios de almacenamiento. Estos métodos suelen llevarse a cabo en una destructora de metal o en una planta de incineración autorizada, con las capacidades específicas para realizar estas actividades de manera eficaz, segura y sin peligro.

Trituración: las trituradoras de papel se pueden utilizar para destruir los medios de almacenamiento flexibles. El tamaño del fragmento de la basura debe ser lo suficientemente pequeño para que haya una seguridad razonable en proporción a la confidencialidad de los datos que no pueden ser reconstruidos.

Los medios ópticos de almacenamiento (CD, DVD, magneto-ópticos) deben ser destruidos por pulverización, trituración de corte transversal o incineración. Cuando el material se desintegra o desmenuza, todos los residuos se reducen a cuadrados de cinco milímetros (5mm) de lado. Como todo proceso de destrucción física, su correcta realización implica la imposibilidad de recuperación posterior por ningún medio conocido. En el caso de los discos duros se deberá asegurar que los platos internos del disco han sido destruidos eficazmente, no sólo la cubierta externa.

Sobre-escritura

La sobre-escritura consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento. La sobre-escritura se realiza accediendo al contenido de los dispositivos y modificando los valores almacenados, por lo que no se puede utilizar en aquellos que están dañados ni en los que no son regrabables, como los CD y DVD.

Todo el procedimiento, así como los plazos de conservación, las técnicas de bloqueo y supresión, deben de ser documentadas por el Responsable.

PRINCIPIO DE RESPONSABILIDAD

Artículo 28. Principios — Responsabilidad.

1. El responsable deberá implementar los mecanismos necesarios para cumplir con los principios, deberes y obligaciones establecidos en esta Ley y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular o al Instituto, según corresponda; observando la Constitución y los Tratados Internacionales en los que el Estado mexicano sea parte; en lo que no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines.

Artículo 29. Principios — Mecanismos de Responsabilidad

1. Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en esta Ley están, al menos, los siguientes:

I. Destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales;

II. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable;

III. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;

IV. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;

V. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;

VI. Establecer procedimientos para recibir y responder dudas y quejas de los titulares;

VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, conforme a esta Ley y demás disposiciones aplicables; y

VIII. 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 con las obligaciones previstas en esta Ley y las demás aplicables.

El responsable debe de diseñar e implementar políticas y programas para protección de datos personales, las cuales deberán de estar aprobadas por el Comité de Transparencia, el Responsable

también deberá de implementar un programa para la revisión periódica de las mismas y cada cuando se actualizan los expedientes del personal.

Se deben de autorizar recursos para la instrumentación de programas y políticas en materia de protección de datos personales, es importante señalar que los recursos no se refieren únicamente a los financieros, sino a recursos materiales, técnicos y humanos.

Por último, la capacitación en materia de protección de datos personales de todo el personal que trate datos, es parte fundamental del principio de responsabilidad. Por lo tanto, los Responsables deben de diseñar un programa de capacitación que señale temporalidad, temas y personal que será capacitado.

MATERIAL DEL REFERENCIA

-  Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.
-  Guía para el Tratamiento de Datos Biométricos.
-  Metodología para la Realización de Verificaciones en Materia de Protección de Datos Personales a Diversos Sujetos Obligados.
-  Medidas Correctivas Generales para los Sujetos Obligados derivadas del Procedimiento de Verificación.
-  Ley de para los Servidores Públicos del Estado de Jalisco.
-  Condiciones Generales de Trabajo del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco y sus Municipios.
-  Ley General de Archivos.
-  Guía sobre borrado seguro de la información. Ciberseguridad, I. N. (s.f.).