Sistema de Gestión de Datos Personales de la Secretaría de Cultura del Poder Ejecutivo del Estado de Jalisco.

El artículo 34 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, establece 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*, se denomina al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

El artículo 65 de los Lineamientos para el Debido Tratamiento de los Datos Personales que deberán Observar los Sujetos Obligados de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, estipula que el *sistema de gestión* deberá permitir planificar, establecer, implementar, operar, monitorear, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales.

En cumplimiento a lo anterior, esta Unidad de Transparencia se avocó a la elaboración del presente documento que contiene el ***SISTEMA DE GESTION***.

GLOSARIO.

I. Comité: Comité de Transparencia de la Coordinación General Estratégica de Desarrollo Social.
II. Coordinación: Coordinación General Estratégica de Desarrollo Social.
III. Enlace de Transparencia: Servidor público responsable de gestionar la información pública al interior de la dependencia de la Unidad Administrativa a la que se encuentra adscrito, o trabajando, en lo relativo a las solicitudes de acceso a la información pública, obligaciones en materia de transparencia y protección de datos personales;

IV. ITEI: El Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco;
V. Ley: La Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios;
VI. Ley General: Ley General de Transparencia y Acceso a la Información Pública;
VII. Ley de Datos Personales: Ley de protección de datos personales en posesión de sujetos obligados del estado de Jalisco y sus Municipios;
VIII. Unidad de Transparencia: Unidad de Transparencia de la Coordinación General Estratégica de Desarrollo Social.
IX. Unidad Administrativa: Sujeto responsable que, en el marco de sus atribuciones y facultades, genera, posee o administra información pública.
X. Secretaría: Secretaría de Cultura del Estado de Jalisco.

OBJETIVO

Los objetivos del presente Sistema de Gestión de Seguridad de Datos Personales son los siguientes:

Establecer las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales en la Secretaría.

Definir el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en la Secretaría.

DE LAS MEDIDAS DE SEGURIDAD:

Uno de los objetivos planteados en este Sistema de Gestión de Seguridad, es documentar las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales implementadas en cumplimiento a la Ley de Datos Personales.

Al respecto, las medidas de seguridad administrativas, físicas y técnicas implementadas en cada uno de los sistemas de tratamiento de datos personales por parte de la Secretaría, son descritas en el *Documento de Seguridad*.

Por tanto, el presente sistema concentrará los resultados, a efecto de estar en oportunidad de planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad vigentes.

MARCO NORMATIVO QUE FACULTA AL SUJETO OBLIGADO RESPONSABLE PARA LA RECOLECCION Y TRATAMIENTO DE DATOS PERSONALES.

Ley General de Transparencia y Acceso a la Información Pública: artículo 70 fracción VII, XI y XVII; y artículo 71; Ley del Servicio Militar: artículo 20; Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios: artículo 8°, párrafo 1, fracción I, incisos j) k) y l); fracción IV inciso e), artículo 25 fracción VII, 31.1 y 32.1 fracciones III y X y artículo 68 fracción II y III; Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco: artículo 51° fracción II, III y IV; Ley para los Servidores Públicos del Estado de Jalisco y sus Municipios, artículo 17 fracción I y XII, 44, 54 Bis-4, 54 Bis-5 56 fracciones XII, XIII y XVIII; Ley de Movilidad y Transporte del Estado de Jalisco: artículo 54; Ley Orgánica del Poder Ejecutivo del Estado de Jalisco: artículo 13 fracción XV; Reglamento Interno de la Coordinación General Estratégica de Desarrollo Social: artículos 5 fracciones XVIII y XX, 13 fracciones I, II, V y VI, 15 fracción IX y 19; Manual de Organización y Procedimientos de la Secretaría de Planeación, Administración y Finanzas (hoy Secretaría de Administración), dentro del Procedimiento denominado ñProcedimiento de Altaò(página 168) y los puntos 4.1, 4.3, 4.11, del 4.59 al 4.69, 6.85, 6.86 y 6.90 de las Políticas Administrativas de la Secretaría de Planeación, Administración y Finanzas (hoy Secretaría de Administración).

En todo tratamiento de datos personales que se realice en la Secretaría, se deberán respetar los principios y deberes dispuestos en la Ley de Datos Personales, asimismo, se deberá privilegiar el interés superior de la niñez, quedando prohibidos los tratamientos que tengan como efecto cualquier tipo de discriminación o señalamiento.

a) Principios que rigen la protección de los datos personales

El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información, y responsabilidad en el tratamiento de los datos personales.

Licitud: Sera 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.

Finalidad: 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 y deberán ser relacionadas con las facultades y atribuciones que la normatividad aplicable les confiera.

Lealtad: 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.

Consentimiento: Cuando no se actualicen algunas de las causales de excepción previstas en la Ley de Protección de Datos personales, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, mismo que podrá ser:

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.

Calidad: 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.

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

Información: 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.

Responsabilidad: El responsable deberá implementar los mecanismos necesarios para cumplir con los principios, deberes y obligaciones establecidos en la Ley de Datos Personales.

b) Deberes que rigen la protección de los datos personales

La Secretaría deberá establecer y mantener 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.

En el respeto de los principios y el cumplimiento de los deberes previstos para el tratamiento de los datos personales, se deberán considerar las etapas que integran el ciclo de vida de los datos personales, las cuales son:

1. Obtención;

2. Uso (registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento divulgación, transferencia o disposición); y,

3. Eliminación.

VISIÓN GENERAL DE LOS PRINCIPIOS Y DEBERES

A efecto de facilitar la comprensión de los principios y deberes en materia de protección de datos personales, cada uno se abordará bajo los aspectos siguientes:

- Breve explicación de la obligación (principio o deber).
- Responsables del cumplimiento.
- Actividades que deberán realizarse para su cumplimiento.
- Medios para acreditar el cumplimiento.

Deber de Seguridad

Debe observarse en todas las etapas del ciclo de vida de los datos personales.

Implementar medidas de seguridad físicas, técnicas y administrativas necesarias para proteger los datos personales contra daño, pérdida, alteración, destrucción, o su uso, acceso o tratamiento no autorizado, así como para garantizar su confidencialidad, integridad y disponibilidad.

Responsables: Todas aquellas áreas que realicen el tratamiento de datos personales.

Cumplimiento: Garantizar la confidencialidad, integridad y disponibilidad de los datos personales, e impedir que el tratamiento respectivo contravenga las disposiciones del marco normativo en la materia.

Ante cualquier modificación de las medidas de seguridad establecidas, las instancias competentes deberán dar aviso a la Unidad de Transparencia, con la finalidad de realizar las modificaciones pertinentes al Documento de Seguridad.

Deber de Confidencialidad: Debe observarse en todas las etapas del ciclo de vida de los datos personales.

Establecer controles o mecanismos para que todas las personas que intervengan en cualquier fase del tratamiento de los datos personales guarden el debido sigilo, obligación que subsistirá aún después de finalizar sus relaciones con el mismo y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

Instancias responsables: Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento: Implementar controles y medidas de seguridad que garanticen el sigilo y la protección de los datos personales.

En caso de elaborar un contrato, establecer cláusulas que obliguen a la confidencialidad de los datos personales a los terceros que intervengan en su tratamiento.

Medios para acreditar el cumplimiento: Evaluando por pate de la Unidad de Transparencia los controles o mecanismos administrativos, técnicos o físicos que se hayan implementado por cada instancia para proteger los datos personales.

Principio de Licitud

Debe observarse en la etapa de **obtención** de los datos personales.

Sera 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.

Instancias responsables: Todas aquellas que se alleguen de datos personales para realizar su tratamiento, en el ámbito de sus respectivas competencias.

Cumplimiento: El aviso de privacidad respectivo deberá incluir de manera precisa el fundamento legal que faculta al sujeto obligado responsable para llevar a cabo la recolección y tratamiento de los datos personales.

Medios para acreditar el cumplimiento: Acreditar que cada tratamiento de datos personales encuentre sustento en las atribuciones o facultades del recolector.

Principio de Lealtad

Debe observarse a lo largo de todo el ciclo de vida de los datos personales.

No obtener ni tratar datos personales a través de medios engañosos y fraudulentos (aquellos que se utilicen para tratar los datos personales con dolo, mala fe o negligencia).

Instancias responsables: Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento: Llevar a cabo el tratamiento de los datos personales únicamente para los fines comunicados al titular en el Aviso de Privacidad.

Medios para acreditar el cumplimiento: La obtención de los datos personales deberá realizarse de manera clara y sencilla, acorde a las atribuciones y facultades de la instancia para realizar el tratamiento.

Poner a disposición de los titulares el Aviso de Privacidad respectivo, para evidenciar que los datos personales obtenidos se utilizarán conforme a lo señalado en el propio aviso y en la normatividad aplicable.

Principio de Información

Debe observarse en la etapa de obtención de los datos personales.

A través del respeto al principio de información, los titulares deberán de conocer las características principales del tratamiento al que serán sometidos sus datos personales.

Instancias responsables: Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento: Previo a la obtención o recepción de los datos personales, poner a disposición del titular el aviso de privacidad.

Los avisos de privacidad deberán contener las características y elementos previstos en la Ley de Datos Personales.

Medios para acreditar el cumplimiento: Deberá ser puesto a disposición de los titulares de manera visible a través de medios físicos y electrónicos que evidencien el cumplimiento a este principio.

Deberán notificar a la Unidad de Transparencia cualquier cambio en el tratamiento de datos personales que requiera una modificación al aviso de privacidad respectivo.

Principio de Consentimiento

Debe observarse en la etapa de obtención de los datos personales.

Para estar en oportunidad de obtener los datos personales y con ello, realizar su tratamiento, **resulta necesario que la instancia cuente con el consentimiento del titular**, salvo que se actualice alguno de los supuestos previstos en la Ley de Datos Personales.

Obligación: Se deberá obtener el consentimiento libre, específico e informado del titular de los datos personales.

El consentimiento podrá manifestarse de forma tácita o expresa.

Instancias responsables: Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento: Identificar si para realizar el tratamiento de los datos personales es necesario el consentimiento de su titular, o si se encuentra dentro de las excepciones previstas en la Ley de Datos Personales.

En caso de que sea necesario recabar el consentimiento del titular, definir el tipo de consentimiento que resulta aplicable (tácito o expreso).

Medios para acreditar el cumplimiento: Las instancias que obtengan o reciban datos personales que se ubiquen en el supuesto de un **consentimiento expreso**, deberán documentar su obtención.

Principio de Proporcionalidad

Debe observarse en la etapa de obtención de los datos personales.

Recibir los datos personales para su tratamiento sólo cuando resulten adecuados, relevantes y necesarios para la finalidad que justifica su obtención.

Se entenderá que los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención, de acuerdo con las atribuciones conferidas a cada instancia por la normatividad que le resulte aplicable.

Instancias responsables: Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento: Cada instancia deberá requerir el mínimo posible de datos personales para lograr las finalidades para las cuales se obtuvieron.

Medios para acreditar el cumplimiento: Los datos personales tratados deberán ser adecuados, relevantes y necesarios para ejercer la facultad o atribución que le permite a la instancia realizar el tratamiento respectivo.

Principio de Finalidad

Debe observarse en la etapa de uso de los datos personales.

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.

En el supuesto de que se requiera realizar un tratamiento de datos personales para **finalidades distintas a las establecidas en el aviso de privacidad**, será necesario que la instancia respectiva cuente con:

1. Atribuciones legales para ello.

2. En caso de que la finalidad no actualice alguno de los supuestos de excepción de la Ley de Datos Personales, contar con el consentimiento del titular.

Instancias responsables: Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento:

1. Identificar las finalidades que no fueron informadas en los avisos de privacidad y que se requieran llevar a cabo.

2. Verificar que existan atribuciones legales y normativas para el tratamiento de los datos personales para estas finalidades adicionales.

Principio de Calidad

Debe observarse en las etapas de uso y eliminación de los datos personales.

Las instancias deberán adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales, principalmente cuando se obtuvieron de manera indirecta del titular.

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

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, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

Instancias responsables: Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento: Para acreditar el cumplimiento del principio de calidad, las instancias deberán implementar acciones y medidas que estimen necesarias y que tengan como objetivo que los datos personales se actualicen y en su caso, corrijan o completen.

Medios para acreditar el cumplimiento: En todo momento, las instancias deberán mantener los datos personales exactos, completos, correctos y actualizados, independientemente del soporte en el que se encuentren (físico o electrónico).

TRANSFERENCIA DE DATOS PERSONALES

Este apartado se refiere a los aspectos que las instancias deberán observar al efectuar una transferencia de datos personales.

Entendiendo como Trasferencia toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado.

Toda transferencia de datos personales sea nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en la Ley de Datos Personales.

Toda transferencia debe encontrarse formalizada mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad aplicable a la Secretaría.

El consentimiento del titular de los datos personales ante transferencias.

Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en la Ley de Datos Personales.

Con excepción de los supuestos siguientes:

1. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:

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.

Formalización de la transferencia.

De conformidad con el artículo 71 de la Ley de Datos Personales, toda transferencia deberá formalizarse mediante alguno de los medios siguientes:

1. Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

2. Lo dispuesto en el párrafo anterior no será aplicable en los siguientes casos:

I. Cuando la transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos; o

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

3. Cuando el responsable decida transferir datos personales a terceros, deberá asegurarse que tal tercero cuenta con políticas y procedimientos acordes a esta Ley, de conformidad con los siguientes criterios:

I. El tercero cuenta con mecanismos para que el interesado pueda informarse sobre el uso y tratamiento que reciben sus datos personales;

II. El tercero cuente con mecanismos para que el titular ejerza sus derechos de acceso, rectificación, cancelación y oposición;

III. El tercero posea medidas de seguridad suficientes que garanticen la protección de los datos personales; y

IV. La transferencia de datos se llevará a cabo con terceros que garanticen un adecuado nivel de cumplimiento de protección de datos.

EJERCICIO DE LOS DERECHOS ARCO

Este apartado se refiere a los aspectos que las instancias deberán considerar ante el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de datos personales.

De conformidad a lo dispuesto por el Artículo 6° y 16° de la Constitución Política de los Estados Unidos Mexicanos; Artículos 45 al 55 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y en acatamiento a lo que dispone los Lineamentos para la Homologación del Ejercicio de Derechos ARCO que Deberán Observar los Sujetos Obligados Previstos por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, los titulares cuentan con los derechos siguientes:

- **Acceso:** es el derecho que tiene el titular de solicitar el acceso a sus datos personales que están en las bases de datos, sistemas, archivos, registros o expedientes del responsable que los posee, almacena o utiliza, así como de conocer información relacionada con el uso que se da a los datos personales.

- **Rectificación:** es el derecho que tiene el titular de solicitar la rectificación o corrección de sus datos personales, cuando éstos sean inexactos o incompletos o no se encuentren actualizados. En ese sentido, puede solicitar a quien posea o utilice sus datos personales que los corrija cuando los mismos sean incorrectos, estén desactualizados o inexactos.

- **Cancelación:** es el derecho que tiene el titular de solicitar que sus datos personales se eliminen de los archivos, registros, expedientes, sistemas, bases de datos del responsable que los posee, almacena o utiliza, cuando ello resulte procedente.

- **Oposición:** es el derecho que tiene el titular de solicitar que sus datos personales no se utilicen para ciertos fines, o de requerir que se concluya el uso de los mismos a fin de evitar un daño a su persona, cuando ello resulte procedente.

El titular de los datos personales podrá solicitar en cualquier tiempo, su Acceso, Rectificación, Cancelación y/u Oposición, mediante la presentación de solicitud de ejercicio de derechos ARCO ante la Unidad de Transparencia de la Coordinación General Estratégica de Desarrollo Social, ubicada en la Avenida Américas 599, edificio Cuauhtémoc, piso 10, Colonia Lomas de Guevara, Guadalajara, Jalisco o a través de la Plataforma Nacional de Transparencia (PNT).

CICLO DE VIDA DE LOS DATOS PERSONALES

Este apartado se refiere a los aspectos que las instancias deberán considerar para determinar el ciclo de vida de los datos personales respecto de los tratamientos que efectúen.

Por lo anterior el diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales, se deberá incluir la identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando su:

- Obtención.
- Almacenamiento.
- Uso.
- Procesamiento.
- Divulgación.
- Retención.
- Destrucción.

Cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados.

De ese modo, en los términos declarados en el Inventario de Datos Personales y Sistemas de tratamiento las instancias deberán realizar lo siguiente:

1. Relacionar las operaciones que integran el tratamiento de los datos personales con las etapas del ciclo de vida.

a) Etapa de obtención: las concernientes a la forma en que se recaban los datos personales.

b) Etapa de uso: aquellas que permiten concretar la finalidad del tratamiento.

c) Etapa de Archivo: las relativas al archivo del documento, en los términos previstos, respectivamente en: la Ley de Archivos del Estado de Jalisco.

d) Etapa de eliminación: las acciones relativas a la baja documental o, en su caso, su destrucción, en los términos señalados en la Ley de Archivos del Estado de Jalisco.

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, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya su plazo de conservación.

El **bloqueo de los datos personales** consiste en 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.

SUPRESIÓN DE DATOS PERSONALES

Este apartado se refiere a los aspectos que las instancias deberán observar al efectuar la eliminación de los datos personales cuando éstos hayan logrado cumplir con su objetivo y entonces puedan finalizar su ciclo de vida.

No obstante, cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, **deberán ser suprimidos**, previo bloqueo en su caso, y una vez que concluya su plazo de conservación.

En el establecimiento de las políticas, métodos y técnicas a que se refiere el párrafo anterior, se deberán considerar los medios de almacenamiento físicos y/o electrónicos en los que se encuentren los datos personales, así como los atributos siguientes:

Irreversibilidad: que el proceso utilizado no permita recuperar los datos personales.

Seguridad y confidencialidad: que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la Ley de Datos Personales.

Amigable al medio ambiente: que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.

EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES.

Cuando el responsable pretenda poner en operación o modificar políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, deberá presentar ante el Instituto una evaluación de impacto a la protección de datos personales.

Una vez recibido el informe, la Unidad de Transparencia analizará que el tratamiento de datos personales efectivamente actualice los supuestos de un tratamiento intensivo o relevante en términos de lo previsto en la Ley de Datos personales, lo que deberá hacer del conocimiento del Comité de Transparencia.

En caso de que se verifique que el supuesto constituye un tratamiento intensivo o relevante, se deberá realizar una evaluación de impacto en la protección de datos personales, y presentarla ante el ITEI con un mínimo de 30 días hábiles previos a la fecha en que se pretenda poner en operación o modificar el tratamiento respectivo.

La Unidad de Transparencia, en coordinación con el área administrativa respectiva, atenderá las observaciones que en su caso realice el ITEI.

CAPACITACIÓN

Este apartado se refiere a la capacitación que deberá otorgarse a los servidores públicos de la Secretaría.

El Comité de Transparencia y la Unidad de Transparencia, deberá establecer un programa anual de capacitación y actualización en materia de protección de datos personales

En ese sentido, a propuesta de la Unidad de Transparencia, el Comité deberá aprobar anualmente el programa de capacitación de datos personales.

INFRACCIONES Y SANCIONES

Serán causas de responsabilidad y sanción por incumplimiento de las obligaciones establecidas en la materia de la Ley de Datos Personales, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO o de la portabilidad de los datos personales;

II. Incumplir los plazos de atención previstos en la Ley de Datos Personales para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;

III. Ampliar con dolo los plazos previstos en la Ley de Datos Personales para responder las solicitudes para el ejercicio de los derechos ARCO o la portabilidad de los datos personales;

IV. 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;

V. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la Ley de Datos Personales;

VI. Mantener los datos personales inexactos cuando resulte imputable al responsable;

VII. No efectuar la rectificación, cancelación u oposición al tratamiento de los datos personales que legalmente proceda, cuando resulten afectados los derechos de los titulares;

VIII. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refieren los artículos 21, 22 y 23 de la Ley de Datos Personales, según sea el caso, y demás disposiciones aplicables;

IX. Clasificar, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en Ley de Transparencia. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;

X. Incumplir el deber de confidencialidad establecido en el artículo 44 de la presente Ley;

XI. No establecer las medidas de seguridad en los términos que establecen los artículos 30, 31, 32, 33, 34, 35 y 36 de la Ley de Datos Personales;

XII. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 30, 31, 37, 42 y 43 de la Ley de Datos Personales;

XIII. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley;

XIV. Obstruir los actos de verificación de la autoridad;

XV. Crear bases de datos personales en contravención a lo dispuesto por la presente Ley;

XVI. No acatar las resoluciones emitidas por el ITEI;

XVII. Aplicar medidas compensatorias en contravención de los criterios que tales fines establezca el Sistema Nacional;

XVIII. Declarar dolosamente la inexistencia de datos personales cuando éstos existan total o parcialmente en los archivos del responsable;

XIX. No atender las medidas cautelares establecidas por el ITEI;

XX. Tratar los datos personales de manera que afecte o impida el ejercicio de los derechos fundamentales previstos en la Constitución Política de los Estados Unidos Mexicanos;

XXI. No cumplir con las disposiciones previstas en los artículos 65, 66, 68 y 69, de la Ley de Datos Personales;

XXII. No presentar ante el Instituto la evaluación de impacto a la protección de datos personales en aquellos casos en que resulte obligatoria, de conformidad con lo previsto en la Ley de Datos Personales y demás normativa aplicable;

XXIII. Realizar actos para intimidar o inhibir a los titulares en el ejercicio de los derechos ARCO; y

XXIV. Omitir la entrega del informe anual a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, de manera extemporánea.

2. Las causas de responsabilidad previstas en las fracciones I, IV, V, IX XII, XIII, XIV XVI, XVIII XX y XXI, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.

3. Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

El presente documento podrá ser actualizado periódicamente, con la finalidad de actualizar los supuestos del Sistema de Gestión de Datos Personales.