TRIBUNAL ADMINISTRATIVO

DEL PODER JUDICIAL DEL ESTADO
CHIAPAS

SISTEMA DE GESTIÓN DE SEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

TRIBUNAL ADMINISTRATIVO DEL PODER JUDICIAL DEL ESTADO DE CHIAPAS

Las suscritas Magistradas Susana Sarmiento López, Mónica de Jesús Trejo Velázquez y el Magistrado Víctor Marcelo Ruiz Reyna, integrantes del Pleno del Tribunal Administrativo del Poder Judicial del Estado, en ejercicio de las facultades que nos confieren los artículos 79, de la Constitución Política del Estado Libre y Soberano de Chiapas; 48 de la de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas; 11, fracción XXXI de la Ley Orgánica y 9, fracciones VIII y XXII del Reglamento Interior ambos ordenamientos del Tribunal Administrativo del Poder Judicial del Estado, y en atención al siguiente:

CONSIDERANDO

Que, en el marco de la materia de Transparencia y Acceso a la Información Pública, existen disposiciones legales que establecen los alcances de la publicidad de los datos, en aras de brindar a la ciudadanía información de utilidad a través de mecanismos y métodos de rendición de cuentas;

Que esas disposiciones son consagradas a través de los artículos 6, apartado A, fracción II, y 16, párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, de éstas se destaca el derecho de petición y/o a ser informado de manera oportuna por las instituciones públicas u órganos de gobierno, así como de personas (físicas o morales) que reciban y ejerzan recursos públicos o que realicen o ejerzan actos de autoridad, con independencia del nivel de gobierno al que pertenezcan.

Lo anterior, garantizando en todo momento el derecho a la Protección de los Datos Personales dentro de los tratamientos a los cuales las personas titulares de los datos proporcionen;

Que, el artículo 34 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en relación con el dispositivo 48 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, establecen que 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; y,

Que, en cumplimiento a lo referido con antelación, la Unidad de Transparencia del Tribunal Administrativo del Poder Judicial del Estado de Chiapas se avocó a la elaboración del Sistema de Gestión de Seguridad en Materia de Protección de Datos Personales, mismo que fue analizado y aprobado de manera preliminar por el Comité de Transparencia con fecha 26 veintiséis de enero de 2023 dos mil veintitrés, de conformidad con el artículo 83, segundo párrafo y 84, fracción I, de la Ley General de Protección, en relación con el numeral 113 de la Ley Estatal de Protección, al ser la autoridad máxima en materia de protección de datos personales, contando con la atribución de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales.

Por los fundamentos y consideraciones anteriormente expuestas, las Magistradas y el Magistrado, integrantes del Pleno del Tribunal Administrativo del Poder Judicial del Estado, tienen a bien expedir el Sistema de Gestión de Seguridad en Materia de Protección de Datos Personales, acorde a lo siguiente:

INDICE

I.- Disposiciones generales

Además de las disposiciones establecidas en el numeral 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el artículo 5 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, en este instrumento se entenderá por:

Área de Informática: a la instancia del Tribunal Administrativo del Poder Judicial del Estado de Chiapas, dependiente de la Unidad de Apoyo Administrativo, encargada de vigilar el cumplimiento de las normas, políticas y procedimientos que en materia de informática establezca el Pleno del Tribunal, conforme a lo señalado en el artículo 64 del Reglamento Interior del Tribunal Administrativo del Poder Judicial del Estado de Chiapas.

Área de Recursos Materiales y Servicios Generales: a la instancia del Tribunal Administrativo del Poder Judicial del Estado de Chiapas, dependiente de la Unidad de Apoyo Administrativo, encargada de implementar las medidas de seguridad necesarias para preservar el patrimonio del Tribunal, conforme a lo señalado en el artículo 62, fracción XXIV del Reglamento Interior del Tribunal Administrativo del Poder Judicial del Estado de Chiapas.

Contraloría: a la instancia del Tribunal Administrativo del Poder Judicial del Estado de Chiapas, encargada de planear, organizar y coordinar el sistema de prevención, control y vigilancia de la administración del Tribunal, que cuenta con autonomía técnica y de gestión para cumplir cabalmente sus atribuciones, señaladas en el artículo 36 y 37 de la Ley Orgánica del Tribunal Administrativo del Poder Judicial del Estado de Chiapas, lo aplicable de la Ley de Responsabilidades Administrativas para el Estado de Chiapas, así como en el Reglamento Interior del Tribunal Administrativo del poder Judicial del Estado de Chiapas.

Grupo Interdisciplinario: al conjunto de personas que coadyuvan en el análisis de los procesos y procedimientos institucionales que dan origen a la documentación, así como en la identificación de los valores

documentales, vigencias, plazos de conservación y disposición documental, durante el proceso de valoración documental del TAPJECH.

ITAIPCH y/u Órgano Garante Local: al Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas.

Ley General de Protección: a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Ley Estatal de Protección: a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

Lineamientos Generales de Protección: a los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Oficial de Protección de Datos Personales: a la persona servidora pública que desempeña las atribuciones señaladas en el artículo 75 Bis del Reglamento Interior del Tribunal Administrativo del Poder Judicial del Estado de Chiapas, con adscripción a la Unidad de Transparencia.

Órganos jurisdiccionales: al Juzgado de Jurisdicción Administrativa, Juzgado Especializado en Responsabilidad Administrativa y a la Sala de Revisión del Tribunal Administrativo del Poder Judicial del Estado de Chiapas.

Órganos administrativos: a las Áreas de carácter administrativo que auxilian en la labor sustancial del Tribunal Administrativo del Poder Judicial del Estado de Chiapas.

Sistema de Gestión: al presente Sistema de Gestión de Seguridad de Protección de Datos Personales del Tribunal Administrativo del Poder Judicial del Estado de Chiapas, consistente en 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 el Tribunal Administrativo del Poder Judicial del Estado de Chiapas.

Titular: a la persona particular o servidora pública titular de los datos personales.

Tribunal Administrativo o TAPJECH: al Tribunal Administrativo del Poder Judicial del Estado de Chiapas.

Unidad de Transparencia: a la Unidad de Transparencia del Tribunal Administrativo del Poder Judicial del Estado de Chiapas.

Unidad de Apoyo Administrativo: al Órgano Administrativo encargado de administrar y controlar el presupuesto de egresos autorizado para cada ejercicio, de acuerdo a la normatividad aplicable, así como para proponer medidas que tiendan a la preservación y al mejoramiento administrativo del Tribunal.

II.- Objetivo

Los objetivos del Sistema de Gestión son los siguientes:

1. Establecer las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales en el TAPJECH.
2. 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 el TAPJECH.

Para ello, se puntualizará el marco legal aplicable, y políticas generales y específicas que deberán regir en el tratamiento de los datos personales. A su vez, se integrará a este documento un Programa de Datos Personales el cual desarrollará los aspectos siguientes:

- Las atribuciones y obligaciones de los órganos jurisdiccionales y administrativos, relacionadas con la protección de los datos personales.
- La visión general de los principios y deberes en la protección de los datos personales.
- Las actuaciones que deben ser consideradas al realizar la transferencia y/o remisión de datos personales.

- Las actuaciones que deben ser consideradas al utilizar el cómputo en la nube.
- Las cuestiones inherentes al ejercicio de los derechos ARCO.
- Las gestiones relativas al derecho de portabilidad de los datos personales.
- La definición del ciclo de vida de los datos personales en el TAPJECH.
- Las cuestiones relacionadas con la supresión de datos personales.
- Las relativas a las Evaluaciones de Impacto ante el ITAIPCH.
- Las inherentes con la capacitación en materia de protección de datos personales.
- Las relacionadas a la revisión y auditoría de las medidas de seguridad de los datos personales.
- El establecimiento de un procedimiento de orientación y quejas relacionadas con el tratamiento de datos personales.
- Acciones para la mejora continua.
- Sanciones aplicables.

III.- 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, de conformidad con lo establecido en el artículo 34 de la Ley General de Protección, en adminiculación con el arábigo 48 de la Ley Estatal de Protección, así como el numeral 65 de los Lineamientos Generales de Protección.

En ese contexto, las medidas de seguridad administrativas, físicas y técnicas operadas por los órganos jurisdiccionales y administrativos del TAPJECH son descritas de manera general en el Documento de Seguridad, el cual incluye los mecanismos que serán operados por la Unidad de Transparencia en conjunto con el Comité de Transparencia del TAPJECH, para su monitoreo, revisión, supervisión y auditoría.

De ese modo, las acciones relacionadas con las medidas de seguridad partirán del análisis de los reportes, dictámenes y directrices que se concluyan de la ejecución de dichos mecanismos.

Por tanto, una vez que los mecanismos sean operados, el presente sistema concentrará los resultados que se desprendan de su realización, a efecto de estar en oportunidad de planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad, de forma que resulten adecuadas para el contexto en que se desenvuelve el tratamiento de los datos personales.

IV.- Marco Normativo

En la protección de datos personales al interior del TAPJECH, resulta aplicable el marco normativo siguiente:

1. Artículos 6, Apartado A, fracción II, y 16, párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos.

2. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

3. Ley General de Transparencia y Acceso a la Información Pública.

4. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

5. Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

6. Lineamientos Generales de Protección de Datos Personales para el Sector Público. (Únicamente a manera de guía e interpretación del presente Sistema de Gestión, así como del Documento de Seguridad).

7. Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales

8. Ley Orgánica del TAPJECH.

9. Reglamento Interior del TAPJECH.

10. Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, con clave CONAIP/SNT/ACUERDO/ORD01-15-12/2017-06, publicado en el Diario Oficial de la Federación de fecha 23 de enero 2018.

11. Código de Ética del TAPJECH.

12. Código de Conducta del TAPJECH.

13. Carta de Confidencialidad del TAPJECH.

14. Criterios de Interpretación en la Elaboración de Versiones Públicas del TAPJECH.

V.- Políticas para la Protección de Datos Personales

En todo tratamiento de datos personales que se realice en el TAPJECH, se deberán respetar los principios y deberes dispuestos en la Ley General de Protección, en relación de la Ley Estatal de Protección, de conformidad con lo estipulado para ello en los Lineamientos Generales de Protección, la Ley Orgánica y el Reglamento Interior, ambos aplicables al TAPJECH, así como la Carta de Confidencialidad, considerando el ciclo de vida de los datos personales.

Lo anterior, en los términos que se explican a continuación.

a) Principios que rigen la protección de los datos personales.

Licitud: El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

Finalidad: Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable le confiera.

Lealtad: La persona responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando 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 el artículo 22 de la Ley General de Protección, en relación con el numeral 18 de la Ley Estatal de Protección, la persona responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales.

Calidad: La persona responsable deberá adoptar las medidas necesarias para mantener exactos, completos, pertinentes, correctos y actualizados los datos personales en su posesión, a fin de que no se altere su veracidad.

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por su titular y hasta que 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.

Proporcionalidad: La persona responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

Información: La persona 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: La persona responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General de Protección, en relación con lo aplicable en la Ley Estatal de Protección.

b) Deberes que rigen la protección de los datos personales.

Los deberes que aplican y que se deben observar para el tratamiento de los datos personales son el de seguridad y el de confidencialidad; el primero, implica que el TAPJECH debe establecer y mantener medidas de carácter administrativo, físico y técnico para la protección de los datos personales en su posesión; mientras que derivado del deber de confidencialidad, se deben definir controles o mecanismos que tengan por objeto que todas aquellas personas servidoras públicas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

c) Generalidades del ciclo de vida de los datos personales.

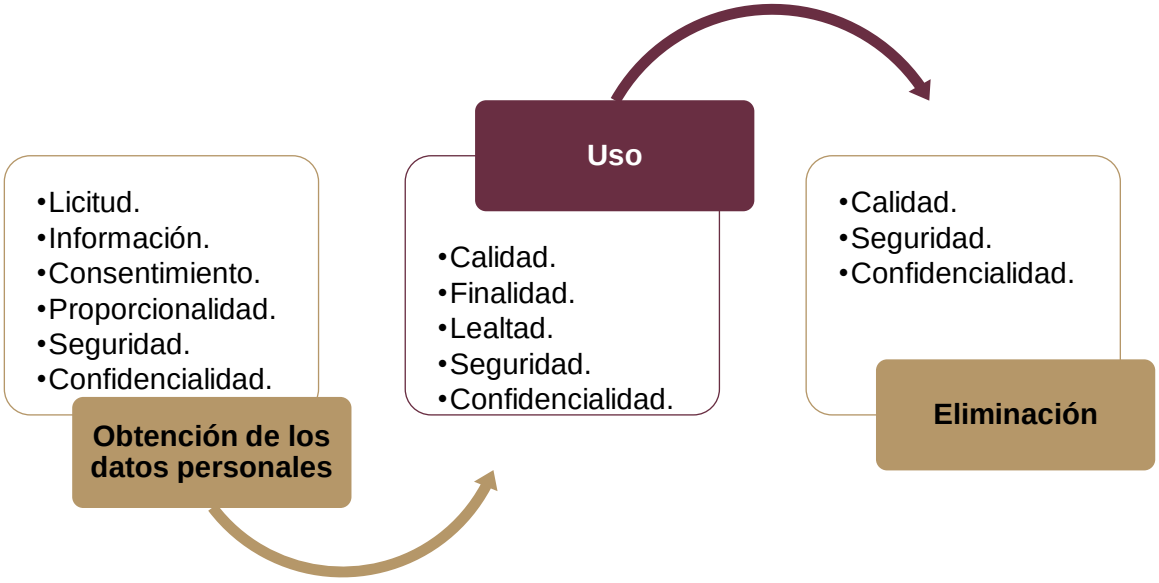
En el respeto a los principios y el cumplimiento de los deberes previstos para el tratamiento de los datos personales, se deberán considerar las etapas que integran su ciclo de vida, las cuales son:

1. Obtención, se refiere a la captura, recepción y/o captación de los datos personales;

2. Uso, pueden ser para: registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición; y,

3. Eliminación, procede cuando los datos personales han cumplido con las finalidades previstas en su tratamiento, pues serán suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

Las etapas del ciclo de vida de los datos personales se concatenan con los principios y deberes de la forma que se indica a continuación:



Por tanto, los órganos jurisdiccionales y administrativos del TAPJECH deberán alinear cada etapa del ciclo de vida de acuerdo al principio y deber respectivo.

d) Prohibición de tratamientos que tengan como efecto cualquier tipo de discriminación.

Queda prohibido el tratamiento de datos personales que tenga como efecto la discriminación de sus titulares por su origen étnico o racial, su estado de salud presente, futuro o pasado, su información genética, sus opiniones políticas, su religión o creencias filosóficas o morales o su preferencia sexual.

e) Privilegiar el interés superior de las niñas, niños y adolescentes. Los órganos jurisdiccionales y administrativos que, en ejercicio de sus funciones realicen el tratamiento de datos personales, deberán privilegiar el interés superior de las niñas, niños y adolescentes, en términos de lo establecido en la Ley General de los Derechos de Niñas, Niños y Adolescentes, así como lo dispuesto en la Ley General de Protección, la Ley Estatal de Protección y los Lineamientos Generales de Protección.

VI.- Atribuciones y obligaciones de los Órganos Jurisdiccionales y Administrativos

Conforme a las disposiciones de la Ley General de Protección, en relación de la Ley Estatal de Protección, corresponde al Comité de Transparencia, a la Unidad de Transparencia y a los órganos jurisdiccionales y administrativos del TAPJECH, la protección, tratamiento y conservación de los datos personales.

En esencia, constituyen las atribuciones y obligaciones siguientes:

Comité de Transparencia	Unidad de Transparencia	Órganos jurisdiccionales y administrativos
Analizar, y en su caso, aprobar las políticas y programas internos de protección de datos personales.	Elaborar las políticas y programas internos de protección de datos personales.	Observar los principios de calidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad y responsabilidad.
Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales.	Establecer un sistema de supervisión de vigilancia para comprobar el cumplimiento de las políticas en materia de datos personales.	Adoptar las medidas necesarias para mantener exactos, completos, pertinentes, correctos y actualizados los datos personales en su posesión.
Supervisar el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.	Documentar el Sistema de Gestión de Seguridad y elaborar el documento de seguridad.	Mantener estricto control sobre los datos personales que obren en sus archivos, teniendo prohibido difundir o realizar un uso no autorizado de los datos personales, incluso finalizado el tratamiento.
Dar vista a la Contraloría del TAPJECH en aquellos casos en que tenga conocimiento de una presunta irregularidad, respecto de determinado tratamiento de datos personales.	Documentar el Plan de Trabajo del TAPJECH, y someterlo a consideración y, en su caso, aprobación del Comité de Transparencia.	

Considerando lo anterior, y con la finalidad de alcanzar los objetivos planteados en el Sistema de Gestión, las políticas y directrices internas de protección de datos personales resultan de observancia obligatoria para todas las personas servidores públicas del TAPJECH que realicen el tratamiento de datos personales.

VII.- Mecanismos para cumplir con los principios y deberes

Para entrar en materia de los principios y deberes materia de protección de datos personales, se describen de la siguiente manera:

1.- Principio de Licitud

1.1.- Aplicación
Debe observarse en la etapa de obtención de los datos personales.

1.2.- Obligación
Sujetar la solicitud y recepción de los datos personales para su tratamiento a las atribuciones o facultades previstas en la Ley Orgánica del TAPJECH, en el Reglamento Interior del TAPJECH, y en las demás disposiciones legales que rigen su actuar.

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

1.4.- Cumplimiento
Identificar la disposición normativa que faculta al órgano jurisdiccional y/o administrativo para realizar el tratamiento de los datos personales, considerando cada una de sus finalidades.

El aviso de privacidad respectivo deberá incluir de manera precisa el fundamento legal que faculte al órgano jurisdiccional y/o administrativo para llevar a cabo el tratamiento correspondiente.

1.5.- Medios para acreditar el cumplimiento
Acreditar que cada tratamiento de datos personales encuentre sustento en las atribuciones o facultades del órgano jurisdiccional y/o administrativo respectivo.

1.6.- Fundamento
Artículos 17 de la Ley General de Protección, 13 de la Ley Estatal de Protección y 8 de los Lineamientos Generales de Protección.

2.- Principio de Lealtad

2.1.- Aplicación
Debe observarse a lo largo de todo el ciclo de vida de los datos personales, desde la obtención, hasta su tratamiento y eliminación.

2.2.- Obligación
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).

Privilegiar la expectativa razonable de privacidad de los titulares evitando que el tratamiento de los datos personales no le provoque discriminación, trato injusto o arbitrario en su contra.

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

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

Verificar que los Avisos de Privacidad respectivos, mantengan un contenido fiel a la realidad del tratamiento de los datos personales, así como que incluyan la totalidad de los elementos previstos para su elaboración en la Ley General de Protección, la Ley Estatal de Protección y los Lineamientos Generales de Protección.

Evitar que el tratamiento de los datos personales provoque a su titular discriminación, trato injusto o arbitrario en su contra.

2.5.- Medios para acreditar el cumplimiento

En el ámbito de su respectiva competencia, los órganos jurisdiccionales y administrativos deberán atender lo siguiente:

a) La obtención de los datos personales deberá realizarse de manera clara y sencilla, acorde a las atribuciones y facultades del órgano jurisdiccional y/o administrativo para realizar el tratamiento.
b) 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.
c) Resguardar la documentación y registros generados durante el tratamiento, de forma que sea posible acreditar que los datos personales se utilizaron conforme a lo señalado en el Aviso de Privacidad y la normatividad aplicable.

2.6.- Fundamento

Artículos 19 de la Ley General de Protección, 16 de la Ley Estatal de Protección y 11 de los Lineamientos Generales de Protección.

3.- Principio de Información

3.1.- Aplicación

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

3.2.- Obligación

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.

Tal conocimiento se concreta a través de la puesta a disposición del aviso de privacidad, que constituye el medio por el que los responsables de los datos personales hacen saber a los particulares la finalidad para la cual se recaba su información.

3.3.- Instancias responsables

Todas aquellas que tengan obligación de emitir el aviso de privacidad.

3.4.- Cumplimiento

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

3.5.- Medios para acreditar el cumplimiento

a) Los avisos de privacidad deberán contener las características y elementos previstos en los artículos 27 y 28 de la Ley General de Protección, 37 y 38 de la Ley Estatal de Protección, y 26 a 41 de los Lineamientos Generales de Protección.

b) Los órganos jurisdiccionales y administrativos competentes deberán verificar que el aviso de privacidad se encuentre:

- Publicado en el portal de internet del TAPJECH.
- Difundido en un medio físico colocado en un lugar visible que facilite su consulta por la/el titular de los datos personales.
- Puesto a disposición del/la titular de forma idónea, esto es, en congruencia con la forma en que los datos personales se obtienen.

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

Se debe realizar un nuevo aviso de privacidad en los casos siguientes:

I. El órgano jurisdiccional y/o administrativo cambie su identidad.

II. Se requiera recabar datos personales sensibles adicionales a aquéllos informados en el aviso de privacidad original, los cuales no se obtengan de manera directa del titular y se requiera de su consentimiento para el tratamiento de éstos.

III. El órgano jurisdiccional y/o administrativo cambie las finalidades señaladas en el aviso de privacidad original.

IV. Se modifiquen las condiciones de las transferencias de datos personales o se pretendan realizar transferencias no previstas inicialmente y el consentimiento del/la titular sea necesario.

3.6.- Fundamento
Artículos 3, fracción II, 26, 27, 28 y 29 de la Ley General de Protección, 5, fracción II, 33, 34, 35, 36, 37, y 38 de la Ley Estatal de Protección y 26 al 45 de los Lineamientos Generales de Protección.

4.- Principio de Consentimiento

4.1.- Aplicación
Debe observarse en la etapa de obtención de los datos personales.

4.2.- Obligación
Para estar en oportunidad de obtener los datos personales y con ello, realizar su tratamiento, resulta necesario que el órgano jurisdiccional y/o administrativo cuente con el consentimiento del/la titular, salvo que se actualice alguno de los supuestos previstos en el artículo 22 de la Ley General de Protección, en relación con el numeral 18 de la Ley Estatal de Protección.

Esto es, en caso de no actualizar alguno de los supuestos previstos en el artículo 22 de la Ley General de Protección, en relación con el numeral 18 de la Ley Estatal de Protección, se deberá obtener el consentimiento libre, especifico e informado del/la titular de los datos personales, de conformidad con lo dispuesto en el artículo 20 de dicha Ley General de Protección, en adminiculación con el numeral 19 de la Ley Estatal de Protección.

El consentimiento podrá manifestarse de forma tácita o expresa.

Por regla general será válido el consentimiento tácito, salvo que la Ley General de Protección o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente.

Para contar con el consentimiento tácito del/la titular de los datos, bastará que habiéndose puesto a su disposición el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

El consentimiento expreso exige que la voluntad del/la titular deba hacerse constar por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.

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

4.4.- 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 General de Protección, y en la Ley Estatal de Protección.

En caso de que sea necesario recabar el consentimiento del/la titular, definir el tipo de consentimiento que resulta aplicable (tácito o expreso). De acuerdo con la forma en que los datos personales son obtenidos (directa o indirectamente del/la titular), establecer la forma y el momento en que debe obtenerse el consentimiento.

En caso de que la o el titular de los datos personales sea un menor de edad, alguien en estado de interdicción o una persona fallecida, identificar y observar las reglas de representación legal que resultan aplicables de acuerdo a la legislación correspondiente.

4.5.- Medios para acreditar el cumplimiento

a) Los órganos jurisdiccionales y administrativos que conforme a sus atribuciones hayan emitido un Aviso de Privacidad, deberán mantener el registro de su publicación, difusión y puesta a disposición.

b) Los órganos jurisdiccionales y administrativos que obtengan o reciban datos personales que se ubiquen en el supuesto de un consentimiento expreso, deberán documentar su obtención.

4.6.- Fundamento
Artículos 20, 21 y 22 de la Ley General de Protección, 18, 19 y 20 de la Ley Estatal de Protección, y 12 al 20 de los Lineamientos Generales de Protección.

5.- Principio de Proporcionalidad

5.1.- Aplicación
Debe observarse en la etapa de obtención de los datos personales.

5.2.- Obligación
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 órgano jurisdiccional y/o administrativo por la normatividad que le resulte aplicable.

Lo anterior, se traduce en que deberán realizarse esfuerzos razonables para limitar los datos personales tratados al mínimo necesario, respecto de las finalidades que motivaron su tratamiento.

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

5.4.- Cumplimiento
Cada órgano jurisdiccional y administrativo deberá identificar los datos personales que se requieren para cada una de las finalidades del tratamiento.

Deberá analizar y revisar que solo se soliciten aquellos que resultan indispensables para cumplir con las finalidades del tratamiento.

Cuando la normativa aplicable establezca con precisión los datos personales que deberán obtenerse para cumplir con la finalidad de que se trate, solo deberán solicitarse dichos datos.

Cada órgano jurisdiccional y administrativo deberá requerir el mínimo posible de datos personales para lograr las finalidades para las cuales se obtuvieron.

5.5.- Medios para acreditar el cumplimiento

Los datos personales tratados deberán ser adecuados, relevantes y necesarios para ejercer la facultad o atribución que le permite al órgano jurisdiccional y/o administrativo realizar el tratamiento respectivo.

5.6.- Fundamento

Artículos 25 de la Ley General de Protección, 31 de la Ley Estatal de Protección y 25 de los Lineamientos Generales de Protección.

6.- Principio de Finalidad

6.1.- Aplicación

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

6.2.- Obligación

Todo tratamiento de datos personales debe estar justificado en razón de finalidades concretas, lícitas, explícitas y legítimas, bajo los conceptos siguientes:

- **Concretas:** cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en la persona titular.
- **Lícitas:** cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades de la persona responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable.
- **Explícitas:** cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.
- **Legítimas:** cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del/la titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General de Protección, en relación con el numeral 18 de la Ley Estatal de Protección.

En todo momento, las finalidades deben estar relacionadas con las atribuciones normativas del órgano jurisdiccional y/o administrativo que realice el tratamiento.

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 el órgano jurisdiccional y/o administrativo respectivo cuente con:

1. Atribuciones legales para ello.
2. En caso de que la finalidad no actualice alguno de los supuestos de excepción del artículo 22 de la Ley General de Protección, en relación del numeral 18 de la Ley Estatal de Protección, contar con el consentimiento del/la titular, salvo que se trate de una persona desaparecida.

Para modificar las finalidades del tratamiento, resultará imprescindible la valoración de los elementos siguientes:

- La expectativa razonable de privacidad del/la titular, basada en la relación que el órgano jurisdiccional y/o administrativo mantiene con éste.
- La naturaleza de los datos personales.
- Las consecuencias para la o el titular que devengan del tratamiento posterior de los datos personales.
- Las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la Ley General de Protección, la Ley Estatal de Protección, y en los Lineamientos Generales de Protección.

6.3.- Instancias responsables

Todas aquellas que realicen el tratamiento de datos personales.

6.4.- Cumplimiento

Se deberá tener presente la finalidad o finalidades de cada tratamiento, y supervisar que las mismas atiendan a fines específicos y determinados, acordes a las atribuciones del TAPJECH.

En todo momento deberá encontrarse identificado el marco normativo que otorga a los órganos jurisdiccionales y administrativos las atribuciones o facultades para tratar los datos personales respecto de cada una de las finalidades.

Resultará indispensable verificar que en los avisos de privacidad se comuniquen todas las finalidades para las cuales se recaban los datos personales y que éstas se describan de manera clara, de modo o forma que el consentimiento del/la titular sea libre, específico e informado.

En caso de que exista la necesidad de tratar datos personales para finalidades distintas a las previstas en el aviso de privacidad, se deberá realizar lo siguiente:

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.
3. Gestionar ante la Unidad de Transparencia la emisión de un nuevo aviso de privacidad, de conformidad con lo establecido en el artículo 44, fracción III de los Lineamientos Generales de Protección y en los términos previstos para el cumplimiento del principio de información en este documento.
4. En caso de que la finalidad quede fuera de los supuestos de excepción del artículo 22 de la Ley General de Protección, en relación del numeral 18 de la Ley Estatal de Protección, solicitar el consentimiento de los titulares para el tratamiento de las finalidades adicionales, mismo que los órganos administrativos deberán realizar en el momento oportuno, es decir, previo a realizar el tratamiento.

6.5.- Medios para acreditar el cumplimiento

Los órganos jurisdiccionales y administrativos deberán acreditar los aspectos siguientes:

- Que los datos personales recabados resulten adecuados, relevantes y necesarios para ejercer la facultad o atribución que le permite realizar el tratamiento respectivo.
- En caso de que el tratamiento de los datos no actualice alguno de los supuestos de excepción previstos en el artículo 22 de la Ley General de Protección, en adminiculación con el numeral 18 de la Ley Estatal de Protección, el órgano jurisdiccional y/o administrativo deberá acreditar haber obtenido el consentimiento del titular posterior a la entrega del aviso de privacidad correspondiente.
- De haberse modificado la finalidad para la que son recabados los datos personales, el órgano jurisdiccional y/o administrativo deberá elaborar o gestionar un nuevo aviso de privacidad a través del cual, dé a conocer a los titulares las nuevas finalidades que atañen al tratamiento de los datos personales.

6.6.- Fundamento

Artículos 18 de la Ley General de Protección, 14 de la Ley Estatal de Protección, 9, 10 y 44, fracción III de los Lineamientos Generales de Protección.

7.- Principio de Calidad

7.1.- Aplicación

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

7.2.- Obligación

Los órganos jurisdiccionales y administrativos 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 entenderá que los datos personales son:

- **Exactos y correctos:** cuando los datos personales no presentan errores que pudieran afectar su veracidad.

- **Completos:** cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del órgano jurisdiccional o administrativo.
- **Actualizados:** cuando se realizan las acciones pertinentes para que los datos personales respondan fielmente a la situación actual 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.

7.3.- Instancias responsables

Todas aquellas que realicen el tratamiento de datos personales.

7.4.- Cumplimiento

Para acreditar el cumplimiento del principio de calidad, los órganos jurisdiccionales y administrativos 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.

Estas medidas deberán permitir que la modificación de los datos personales sea inmediata, una vez que se tenga conocimiento de la actualización o corrección a que haya lugar.

7.5.- Medios para acreditar el cumplimiento

- En todo momento, los órganos jurisdiccionales y administrativos deberán mantener los datos personales exactos, completos, correctos y actualizados, independientemente del soporte en el que se encuentren (físico o electrónico).
- De haber resultado procedente la rectificación de los datos personales, los órganos jurisdiccionales y administrativos, deberán conservar las constancias o anotaciones respectivas.

7.6.- Fundamento
Artículos 23 y 24 de la Ley General de Protección, 27 y 28 de la Ley Estatal de Protección, 21 y 22 de los Lineamientos Generales de Protección.

8.- Deber de seguridad

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

8.2.- Obligación
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.

Las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

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

8.4.- Cumplimiento
Implementar las medidas de seguridad que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado; las cuales podrán ser de carácter administrativo, físico y técnico.

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, los órganos jurisdiccionales y administrativos competentes deberán dar aviso a la Unidad de Transparencia, con la finalidad de realizar las modificaciones pertinentes al Documento de Seguridad del TAPJECH.

Asimismo, establecer mecanismos para asegurar que los servidores públicos involucrados en el tratamiento conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.

8.5.- Medios para acreditar el cumplimiento
Evidencia generada por cada órgano jurisdiccional y administrativo respecto de la implementación de las directrices, controles, mecanismos y procedimientos de seguridad previstos en el Documento de Seguridad del TAPJECH.

8.6.- Fundamento
Artículos 31, 32, 33, 34, 35 y 36 de la Ley General de Protección, 45, 46, 47, 48, 49, 50 y 51 de la Ley Estatal de Protección, y 55 al 65 de los Lineamientos Generales de Protección.

9.- Deber de confidencialidad

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

9.2.- Obligación
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.

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

9.4.- 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.

9.5.- Medios para acreditar el cumplimiento

a) Atento a la atribución conferida al Área de Recursos Humanos, relativa a operar mecanismos de administración del personal del TAPJECH, dicha Área se encontrará obligada de hacer del conocimiento de toda persona a quien se le confiera un empleo, cargo o comisión, el deber de confidencialidad que debe guardar respecto del tratamiento de los datos personales que realice en ejercicio de las funciones que le son concedidas.

   Lo anterior, se realizará a través de la inscripción en el nombramiento respectivo, de la leyenda siguiente:

   "Se hace del conocimiento de la persona servidora pública que, de conformidad con el artículo 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en relación con el numeral 57 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, deberá guardar confidencialidad respecto de los datos personales que sean tratados en ejercicio de las funciones que le son conferidas, obligación que subsistirá aún después de finalizar su relación laboral con el TAPJECH.

   Lo anterior, sin menoscabo de lo establecido en las disposiciones de acceso a la información pública."

   Dicha acción es complementaria y robustece la suscripción de las disposiciones contenidas en la Carta de Confidencialidad que toda persona servidora pública observa en su actuar hacia el TAPJECH.

b) Controles o mecanismos administrativos, técnicos o físicos que se hayan implementado por cada órgano administrativo y jurisdiccional para proteger los datos personales.

9.6.- Fundamento

Artículos: 42 de la Ley General de Protección, 57 de la Ley Estatal de Protección y 71 de los Lineamientos Generales de Protección.

VIII.- De la transferencia de datos personales

Este apartado se refiere a los aspectos que los órganos jurisdiccionales y administrativos deberán observar al efectuar una transferencia de datos personales.

A) Aspectos Generales

Por transferencia debe entenderse todo traslado de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de:

- Su titular.
- El TAPJECH.
- Los encargados - que en su caso sean - contratados por el TAPJECH.

De los artículos 65 y 66 de la Ley General de Protección, en relación con los numerales 94 y 96 de la Ley Estatal de Protección se desprenden dos reglas aplicables a las transferencias de datos personales:

1. Toda transferencia de datos personales sea nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de la Ley General de Protección, en adminiculación de los arábigos 18, 95 y 96 de la Ley Estatal de Protección.

2. 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 al TAPJECH, con excepción de los supuestos previstos en el artículo 66 de la Ley General de Protección, en relación con el numeral 95 de la Ley Estatal de Protección.

A continuación, se abundará sobre dichas reglas generales y sus excepciones correspondientes.

B) 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 los artículos 22, 66 y 70 de la Ley General de Protección, en adminiculación de los arábigos 18, 95 y 96 de la Ley Estatal de Protección.

Lo anterior implica que, los órganos jurisdiccionales y administrativos deben contar con el consentimiento del titular de los datos personales para realizar transferencias. Con excepción de los supuestos siguientes:

- Cuando la transferencia esté prevista en la Ley General de Protección u otras leyes, convenios o tratados internacionales suscritos y ratificados por México.
- Cuando la transferencia se realice entre el TAPJECH y otro responsable, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.
- Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia.
- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última.
- Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados.
- Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el TAPJECH y el titular de los datos personales.
- Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el TAPJECH y un tercero.

- Cuando se trate de los casos en los que el TAPJECH no está obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 22 de la Ley General de Protección, en relación con el numeral 18 de la Ley Estatal de Protección.
- Cuando la transferencia sea necesaria por razones de seguridad nacional.

Bajo el esquema expuesto, si la transferencia a realizar se encuentra sujeta al consentimiento del titular de los datos personales, los órganos jurisdiccionales y administrativos deberán realizar las gestiones necesarias para recabarlo.

Al respecto, de conformidad con el artículo 113 de los Lineamientos Generales de Protección, por regla general el consentimiento a que se refiere el punto anterior será **tácito**, salvo que una ley exija al TAPJECH recabar el consentimiento expreso para la transferencia de sus datos personales.

En términos de lo previsto en el artículo 114 de los Lineamientos Generales de Protección, cuando se requiera el consentimiento **expreso**, el órgano jurisdiccional y/o administrativo podrá establecer cualquier medio lícito que le permita obtenerlo de manera previa a la transferencia de los datos personales.

En todos los casos, los órganos jurisdiccionales y administrativos deberán verificar que en el aviso de privacidad correspondiente al tratamiento en que los datos personales fueron recabados, se realice lo siguiente:

- Se informe al titular de la transferencia a realizar.
- Se implementen los mecanismos y medios disponibles para que la/el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren su consentimiento, de conformidad con el artículo 27, fracción IV, de la Ley General de Protección, en relación del numeral 37, fracción IV de la Ley Estatal de Protección.

En términos del artículo 113 de los Lineamientos Generales de Protección, el TAPJECH deberá comunicar al destinatario o receptor de los datos personales, el aviso de privacidad conforme al cual se obligó a tratar los datos personales frente al titular.

C) Formalización de la transferencia.

De conformidad con el artículo 66 de la Ley General de Protección, en adminiculación con el numeral 96 de la Ley Estatal de Protección, toda transferencia deberá formalizarse mediante alguno de los medios siguientes:

- Suscripción de cláusulas contractuales.
- Convenios de colaboración.
- Instrumentos jurídicos que de conformidad con la normatividad que resulte aplicable, permitan demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

Dicha formalización no será aplicable en los casos siguientes:

- 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.
- 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 aquéllas que dieron origen al tratamiento del responsable transferente.

Bajo ese panorama, si la transferencia no se ubica en ninguno de las excepciones referidas, previo a la realización de una transferencia de datos personales, los órganos jurisdiccionales y administrativos deberán realizar lo siguiente:

- Identificar las cláusulas contractuales, convenios de colaboración o instrumentos jurídicos existentes en que se encuentren previstas las transferencias de los datos personales.
- Verificar que, en dichas cláusulas contractuales, convenios o instrumentos, se refleje el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.
- Comunicar al tercero receptor el aviso de privacidad correspondiente al tratamiento en que se obtuvieron los datos personales.
- Solicitar al tercero receptor que manifieste por escrito que se obliga a proteger los datos personales conforme a los principios y deberes que establece la Ley General de Protección, la Ley Estatal de Protección y las disposiciones que resulten aplicables en la materia.

Respecto del punto anterior, es importante considerar que en términos del artículo 116 de los Lineamientos Generales de Protección, el TAPJECH sólo podrá transferir datos personales fuera del territorio nacional cuando el receptor o destinatario se obligue a proteger los datos personales conforme a los principios, deberes y demás obligaciones similares o equiparables a las previstas en la Ley General y demás normatividad mexicana en la materia, así como a los términos previstos en el aviso de privacidad que le será comunicado por el responsable transferente.

En caso de considerarlo necesario, los órganos jurisdiccionales y administrativos podrán solicitar a través de la Unidad de Transparencia la gestión ante el órgano garante competente, de una opinión respecto de la logística de la realización de aquellas transferencias internacionales de datos personales que pretendan efectuarse; por lo que deberá de cumplirse con el procedimiento estipulado en el artículo 117 de los Lineamientos Generales de Protección.

Lo anterior, de conformidad con lo establecido en los artículos 65, 66, 67, 68, 69, 70 y 71 de la Ley General de Protección, en relación con los numerales 94, 95, 96, 97 y 98 de la Ley Estatal de Protección y 113 a 118 de los Lineamientos Generales de Protección.

IX.- Remisión de Datos Personales

Este apartado se refiere a los aspectos que los órganos jurisdiccionales y administrativos deberán observar al efectuar una remisión de datos personales.

Aspectos Generales

La remisión se refiere a toda comunicación de datos personales realizada exclusivamente entre el TAPJECH y una persona ajena que sola o conjuntamente con otras, efectuará el tratamiento datos personales a nombre y por cuenta del propio Tribunal Administrativo.

Para efectos de la remisión de datos personales, la persona ajena que sola o de forma conjunta con otras efectúe el tratamiento, se le denominará encargado.

Al respecto, de conformidad con los artículos 59, 60, 61 y 62 de la Ley General de Protección, en relación con los numerales 86, 87, 88, 89 y 90 de la Ley Estatal de Protección, así como los diversos 108, 109 y 110 de los Lineamientos Generales de Protección, los órganos jurisdiccionales y administrativos deberán formalizar su relación con los encargados mediante un contrato o instrumento jurídico que permita acreditar su existencia, alcance y contenido.

Dicho contrato o instrumento deberá considerar con carga al encargado, al menos, las obligaciones siguientes:

- Realizar el tratamiento de los datos personales conforme a la normativa del TAPJECH y a las instrucciones que, en su caso, se indiquen en el contrato o instrumento jurídico respectivo.

- Abstenerse de tratar los datos personales para finalidades distintas a las establecidas en la normativa del TAPJECH o de lo instruido en el contrato o instrumento jurídico respectivo.
- Implementar medidas de seguridad conforme a la Ley General de Protección, Ley Estatal de Protección, Lineamientos Generales de Protección, y los instrumentos jurídicos aplicables.
- Informar inmediatamente sobre la vulneración de datos personales al órgano jurisdiccional y/o administrativo del TAPJECH con quien se haya realizado la remisión de estos.
- Durante y después de la transmisión de los datos personales, deberán guardar la confidencialidad respecto de los mismos.
- Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el TAPJECH, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
- Abstenerse de transferir los datos personales salvo en el caso de que el TAPJECH así lo determine, o la comunicación derive de una subcontratación, o bien, se realice por mandato expreso de la autoridad competente.
- Permitir y colaborar con el TAPJECH o con el Órgano Garante Local competente, para realizar verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales, o en su caso, proporcionar la documentación o información que se estime necesaria.
- Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de todas las obligaciones.

En mérito de lo anterior, los órganos administrativos que, en el ámbito de su competencia, realicen contrataciones que impliquen el tratamiento de datos personales por parte de encargados, deberán formalizar tales relaciones mediante un contrato o instrumento jurídico que contenga las obligaciones y cláusulas antes señaladas, incluyendo aquella que regule lo que procederá en caso de que el encargado desee subcontratar servicios que involucren el tratamiento de datos personales.

En términos de lo previsto en el artículo 60 de la Ley General de Protección, en relación con el numeral 88 de la Ley Estatal de Protección, cuando el encargado incumpla las instrucciones del TAPJECH y decida por sí mismo sobre el tratamiento de los datos personales, asumirá el carácter de responsable conforme a la legislación de la materia que le resulte aplicable.

- **Apartado especial sobre la regulación de las subcontrataciones dentro de la remisión de datos personales.**

Como se indicó, el contrato o instrumento jurídico en que se convenga la remisión, deberá incluir la regulación procedente en caso de que el encargado desee subcontratar servicios que involucren el tratamiento de los datos personales.

En todos los casos, los órganos jurisdiccionales y administrativos competentes deberán conocer y autorizar las subcontrataciones que el encargado realice.

Las autorizaciones se podrán otorgar desde el contrato original, cuando el encargado ya prevea subcontrataciones específicas y garantice que las mismas se realizarán en las condiciones precisadas. En caso contrario, la autorización se podrá realizar de manera posterior.

Para ello, el contrato o instrumento jurídico deberá establecer que las subcontrataciones que no se establezcan de manera expresa en dicho contrato o instrumento, deberán ser autorizadas por el TAPJECH previo a su ejecución.

Asimismo, se deberá comunicar al encargado que el contrato o el instrumento jurídico mediante el cual se formalice la subcontratación deberá incluir cláusulas con las obligaciones indicadas.

X.- Cómputo en la Nube

Este apartado se refiere a los aspectos que los órganos administrativos deberán observar al contratar servicios de cómputo en la nube.

Cómputo en la nube, se refiere a un 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 virtuales en recursos compartidos dinámicamente.

En términos de los artículos 63 y 64 de la Ley General de Protección, en relación con los numerales 91 y 92 de la Ley Estatal de Protección, los órganos administrativos podrán contratar o adherirse a servicios, aplicaciones e infraestructura de cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice las políticas de protección de datos personales equivalentes a los principios, deberes, obligaciones y responsabilidades establecidas en la Ley General de Protección, Ley Estatal de Protección, los Lineamientos Generales de Protección y demás disposiciones que resulten aplicables en la materia.

En caso de que el TAPJECH contrate dichos servicios, deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos.

Por otro lado, en el supuesto de que el TAPJECH se adhiera a dichos servicios mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente:

- Tener y aplicar políticas de protección de datos personales afines a los principios y deberes que establecen la Ley General de Protección, la Ley Estatal de Protección, los Lineamientos Generales de Protección y demás normativa aplicable.
- Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio.

- Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio.
- Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.
- Además, se deberá verificar que el proveedor cuente con mecanismos, al menos, para:

a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta.

b) Permitir al TAPJECH limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio.

c) Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio.

d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al TAPJECH y que este último haya podido recuperarlos.

e) Impedir el acceso a los datos personales a personas que no cuenten con permisos de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al TAPJECH.

En ningún caso, el TAPJECH podrá adherirse a servicios que no garanticen la debida protección de los datos personales, conforme a la Ley General de Protección, Ley Estatal de Protección, Lineamientos Generales de Protección, y demás disposiciones que resulten aplicables en la materia.

Es importante referir que, de conformidad con el artículo 111 de los Lineamientos Generales de Protección, los proveedores de servicios de cómputo en la nube tendrán el carácter de encargados, por lo que el órgano administrativo que pretenda contratar sus servicios deberá verificar el cumplimiento de lo estipulado en el capítulo de este sistema denominado “Remisión de datos personales”; es decir, además de

observar las obligaciones señaladas, deberá incluir en el contrato o instrumento jurídico las obligaciones generales de cualquier encargado, las cuales son:

- Realizar el tratamiento de los datos personales conforme a la normativa del TAPJECH y a las instrucciones que, en su caso, se indiquen en el contrato o instrumento jurídico respectivo.
- Abstenerse de tratar los datos personales para finalidades distintas a las establecidas en la normativa del TAPJECH y de lo instruido en el contrato o instrumento jurídico respectivo.
- Implementar medidas de seguridad conforme a la Ley General de Protección, Ley Estatal de Protección, Lineamientos Generales de Protección, y los instrumentos jurídicos aplicables.
- Informar al órgano jurisdiccional y/o administrativo del TAPJECH con quien se haya realizado la remisión de los datos personales cuando ocurra una vulneración a estos.
- Guardar confidencialidad respecto de los datos personales tratados.
- Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el TAPJECH, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
- Abstenerse de transferir los datos personales salvo en el caso de que el TAPJECH así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
- Permitir y colaborar con el TAPJECH o con el organismo garante competente, para realizar verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales, o en su caso, proporcionar la documentación o información que se estime necesaria.
- Generar, actualizar y conservar la documentación necesaria que le permita acreditar y verificar el cumplimiento de todas las obligaciones.

XI.- Relativo al Ejercicio de los Derechos ARCO

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

De conformidad con los artículos 43 al 56, 85, fracción II y 86 de la Ley General de Protección, en relación con los numerales 59 al 84, 117, fracción II y 119 de la Ley Estatal de Protección, y 73 al 107 de los Lineamientos Generales de Protección, las personas titulares cuentan con los derechos siguientes:

- **Acceso:** es el derecho que tiene la persona 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 la persona 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 la persona 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 la persona 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 trámite de las solicitudes de ejercicio de los derechos referidos, será substanciado por la Unidad de Transparencia, en términos de lo establecido en la Ley General de Protección, la Ley Estatal de Protección y los Lineamientos Generales de Protección.

XII.- De la Portabilidad de los Datos Personales

Este apartado se refiere a los aspectos que los órganos administrativos deberán observar ante el ejercicio del derecho de portabilidad.

a) Aspectos Generales

La portabilidad constituye un derecho de las personas titulares que tiene por objeto la reutilización de sus datos personales.

A través del ejercicio de la portabilidad, las personas titulares pueden recibir los datos personales que han proporcionado a un responsable y transmitirlos a otro responsable, siempre y cuando los datos personales se encuentren en un formato estructurado, de uso común y lectura mecánica.

Lo anterior bajo las consideraciones establecidas en la Ley General de Protección, la Ley Estatal de Protección, así como el presente apartado.

b) Ejercicio del derecho de Portabilidad

En términos de lo previsto en el artículo 57 de la Ley General de Protección, en relación con el numeral 85 de la Ley Estatal de Protección el titular podrá ejercer el derecho de portabilidad cuando el tratamiento de los datos personales cuente con las características siguientes:

1. Se realice vía electrónica;
2. Tenga un formato estructurado y comúnmente utilizado; y,
3. La persona titular hubiere proporcionado directamente al TAPJECH sus datos personales de forma activa y consciente.

De modo que, de actualizarse los supuestos citados, la persona titular tendrá derecho a transmitir sus datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado, a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales.

En términos del artículo 8 de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, se entenderá que un formato adquiere la calidad de estructurado y comúnmente utilizado, con independencia del sistema informático utilizado para su generación y reproducción, cuando se cumplan los supuestos siguientes:

I. Se trate de un formato electrónico accesible y legible por medios automatizados, de tal forma que éstos puedan identificar, reconocer, extraer, explotar o realizar cualquier otra operación con datos personales específicos;
II. El formato permita la reutilización y/o aprovechamiento de los datos personales; y,
III. El formato sea interoperable con otros sistemas informáticos, esto es, que el TAPJECH y el órgano administrativo receptor tengan la capacidad de compartir infraestructura y datos personales a través de la conexión de sus respectivos sistemas o plataformas tecnológicas.

Bajo ese esquema, atento a lo previsto en el artículo 7 de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, la portabilidad de los datos personales ante el TAPJECH, tendrá por objeto que la persona titular pueda solicitar:

- Una copia de los datos personales que hubiere facilitado directamente a un órgano administrativo, en un formato estructurado y comúnmente utilizado, que le permita seguir utilizándolos y, en su caso, entregarlos a un órgano administrativo diverso del TAPJECH para su reutilización y aprovechamiento en un nuevo tratamiento.
- La transmisión de sus datos personales a un órgano administrativo receptor diverso del TAPJECH, siempre y cuando sea técnicamente posible, la persona titular hubiere facilitado directamente sus datos personales al órgano administrativo transmisor y el tratamiento de éstos se base en su consentimiento o en la suscripción de un contrato.

c) Trámite del ejercicio de Portabilidad

De conformidad con los artículos 14 y 27, fracción I de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, en relación con los numerales 51, 52, octavo párrafo de la Ley General de Protección; 73, primer párrafo y 74 de la Ley Estatal de Protección, la atención de las solicitudes de portabilidad de los datos personales se realizará a través de la Unidad de Transparencia del TAPJECH.

El trámite respectivo será efectuado de conformidad con las reglas específicas para el ejercicio de la portabilidad y las normas técnicas y procedimientos para la transmisión de datos personales, estipuladas en los capítulos III y IV de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, así como lo establecido en la Ley General de Protección, Ley Estatal de Protección, Lineamientos Generales de Protección.

Por lo anterior, en caso de que alguno de los órganos jurisdiccionales o administrativos del TAPJECH reciba una solicitud de ejercicio del derecho de portabilidad de los datos personales, deberán remitirla a la Unidad de Transparencia al día hábil siguiente a su recepción.

XIII.- Del ciclo de vida de los Datos Personales

Este apartado se refiere a los aspectos que los órganos jurisdiccionales y administrativos deberán considerar para determinar el ciclo de vida de los datos personales respecto de los tratamientos que efectúen.

De conformidad con el artículo 33, fracción I de la Ley General de Protección, y en relación con el numeral 47, fracción I de la Ley Estatal de Protección, para establecer y mantener las medidas de seguridad para la protección de los datos personales, se deberán crear políticas internas para su gestión y tratamiento que consideren el contexto en el que ocurren los tratamientos, así como el ciclo de vida de los datos personales; es decir, su obtención, uso y posterior eliminación.

Debido a ello, la fracción IV, del artículo 56 de los Lineamientos Generales de Protección, señala que, en 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.

Para definir el ciclo de vida de los datos personales, se deberá partir de las etapas que se representan en el esquema siguiente:

Etapas del ciclo de los datos personales

De ese modo, en los términos que se declararán en el Inventario de Datos Personales y Sistemas que realizarán los órganos jurisdiccionales y administrativos, según cada tratamiento, se acotarán 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, bajo los términos que determine cada órgano jurisdiccional y administrativo, acorde a los ordenamientos aplicables en la materia, y según los parámetros y criterios que se estipulen bajo acuerdos del Grupo Interdisciplinario del TAPJECH.

d) **Etapa de eliminación:** las acciones relativas a la baja documental o, en su caso, su destrucción, en los términos que se estipulen bajo acuerdos del Grupo Interdisciplinario del TAPJECH.

2. Definidas las etapas que preceden, el ciclo de vida de los datos personales de cada tratamiento estará determinado.

De conformidad con el artículo 24 de la Ley General de Protección, en relación con el numeral 30 de la Ley Estatal de Protección, 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 una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con el periodo de su tratamiento, hasta que concluya el plazo de vigencia documental o en su caso, de prescripción legal. Periodo en el que, los datos personales no podrán ser objeto de tratamiento.

Una vez transcurrido el bloqueo de los datos personales, procederá su eliminación, de conformidad con el procedimiento de baja archivística que los órganos jurisdiccionales y administrativos en conjunto del Área Coordinadora de Archivos del TAPJECH prevean para dicho propósito.

Al respecto, el bloqueo de los datos personales corresponderá a los periodos máximos de vigencia documental, o en su caso, a los plazos de conservación, que se establezcan por común acuerdo dentro de lo general, así como en lo particular los órganos jurisdiccionales y administrativos parte del Grupo Interdisciplinario del TAPJECH.

Cada órgano jurisdiccional y/o administrativo deberá mantener identificado el ciclo de vida de los datos personales y el periodo de bloqueo de la totalidad de los tratamientos que efectúen en ejercicio de sus funciones.

Tal identificación, deberá ser verificada por la Unidad de Transparencia a través de las funciones de supervisión que le son encomendadas en el Documento de Seguridad y el presente Programa de Protección de Datos Personales.

XIV.- Supresión de los Datos Personales

Este apartado se refiere a los aspectos que los órganos jurisdiccionales y administrativos 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.

En términos de lo establecido en el artículo 23 de la Ley General de Protección, en relación con el numeral 27, primer párrafo de la Ley Estatal de Protección, se deberán adoptar las medidas necesarias para mantener los datos personales exactos, completos, correctos y actualizados, a fin de que no se altere su veracidad.

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.

Al respecto, el artículo 23 de la Ley General de Protección, en relación con el numeral 27, primer párrafo de la Ley Estatal de Protección, señalan que se deberán establecer políticas, métodos y técnicas

orientadas a la supresión definitiva de los datos personales, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.

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 en la Ley General de Protección, la Ley Estatal de Protección y Lineamientos Generales de Protección.
- **Favorables al medio ambiente:** que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.

Atendiendo a lo que precede, los órganos jurisdiccionales y administrativos deberán suprimir los datos personales de conformidad con lo que se expone a continuación.

a) Supresión de los datos personales en órganos administrativos

Las unidades/áreas administrativas, acorde a lo que se establezca de manera general y en lo particular, conforme a las determinaciones en conjunto con el Grupo Interdisciplinario, deberán realizar lo siguiente:

1. Mantener identificados los plazos de conservación de las series y subseries documentales que contienen datos personales.
2. Realizar la destrucción de los documentos correspondientes a dichas series y subseries documentales cuando haya concluido el plazo de conservación respectivo.
3. Supervisar que la referida destrucción, se efectúe considerando los atributos de irreversibilidad, seguridad, confidencialidad y favoreciendo al medio ambiente.

Cabe indicar que, relativo a los documentos electrónicos, aquellos en los que los órganos administrativos utilicen la firma electrónica avanzada, se les dará el mismo tratamiento archivístico que si se tratase de un documento en papel, en cuanto a su organización, descripción, vigencia y plazos de conservación. Ello, en el entendido de que los documentos electrónicos se refieren a los que los órganos administrativos utilicen la firma de mérito, para efectuar trámites o proporcionar servicios que impliquen la certificación de las personas en lo particular.

b) Supresión de los datos personales en órganos jurisdiccionales.

Conforme a las determinaciones que tengan a bien considerar la persona titular del órgano respectivo, en conjunto con el Grupo Interdisciplinario del TAPJECH, relativo a las disposiciones en materia de valoración, depuración, destrucción, digitalización, transferencia y resguardo de los expedientes judiciales generados por los órganos jurisdiccionales, éstos últimos deberán realizar lo siguiente:

1. Mantener identificados los plazos de conservación de las series y subseries documentales que contienen datos personales.

2. Realizar la depuración o destrucción de los documentos respectivos.

3. Supervisar que la depuración o destrucción, se efectúe considerando los atributos de irreversibilidad, seguridad, confidencialidad y favoreciendo al medio ambiente.

XV.- Evaluación de impacto en la protección de Datos Personales

Este apartado se refiere a los aspectos que los órganos administrativos deberán observar al pretender implementar un tratamiento intensivo o relevante de los datos personales, caso en el que será procedente solicitar una evaluación de impacto ante el Órgano Garante Local de la materia.

a) Aspectos generales.

En términos de lo estipulado en el artículo 74 de la Ley General de Protección, en relación con el numeral 103 de la Ley Estatal de Protección, cuando se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio implique el tratamiento intensivo o relevante de datos personales, se deberá realizar una evaluación de impacto en la protección de datos personales, y presentarla ante el Órgano Garante Local de la materia, quien podrá emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

b) Tratamiento intensivo o relevante de los datos personales.

De conformidad con lo señalado en los artículos 75 y 76 de la Ley General de Protección, en adminiculación con el numeral 104 de la Ley Estatal de Protección, y el dispositivo 8 del Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales[1] (en adelante Acuerdo de Evaluaciones de Impacto), se estará en presencia de un tratamiento intensivo o relevante de datos personales cuando ocurra uno los siguientes supuestos:

I.- Existan riesgos inherentes a los datos personales a tratar, entendidos como el valor potencial cuantitativo o cualitativo que pudieran tener éstos para una tercera persona no autorizada para su posesión o uso en función de la sensibilidad de los datos personales; las categorías de titulares; el volumen total de los datos personales tratados; la cantidad de datos personales que se tratan por cada titular; la intensidad o frecuencia del tratamiento, o bien, la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas;

[1] Acuerdo publicado en el Diario Oficial de la Federación de fecha 23 de enero de 2018.

II. Se traten datos personales sensibles a los que se refiere el artículo 3, fracción X de la Ley General de Protección, en relación con el numeral 5, fracción IX de la Ley Estatal de Protección, entendidos como 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 mas no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual; y

III. Se efectúen o pretendan efectuar transferencias de datos personales a las que se refiere el artículo 3, fracción XXXII de la Ley General de Protección, en relación con el diverso 5, fracción XXXIV de la Ley Estatal de Protección, entendidas como cualquier comunicación de datos personales, dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado, considerando con especial énfasis, de manera enunciativa mas no limitativa, las finalidades que motivan éstas y su periodicidad prevista; las categorías de titulares; la categoría y sensibilidad de los datos personales transferidos; el carácter nacional y/o internacional de los destinatarios o terceros receptores y la tecnología utilizada para la realización de éstas.

c) Evaluación de Impacto.

Consiste en la valoración de las consecuencias reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares de los datos personales, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

Los órganos jurisdiccionales y administrativos que pretendan implementar o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio implique el tratamiento intensivo o relevante de datos personales, 45 días hábiles previos a la fecha en que se considere poner en operación, deberán emitir un informe dirigido a la Unidad de Transparencia que dé cuenta de los aspectos siguientes:

- La descripción de la política, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales que pretenda poner en operación o modificar.
- La justificación de la necesidad de tal implementación o modificación.
- La representación del ciclo de vida de los datos personales a tratar.
- La identificación, análisis y descripción de la gestión de los riesgos inherentes para la protección de los datos personales.
- El análisis de cumplimiento normativo en materia de protección de datos personales de conformidad con la Ley General de Protección, la Ley Estatal de Protección y la normativa aplicable.
- Cualquier otra información o documentos que se considere conveniente.

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 General de Protección, la Ley Estatal de Protección y en el Acuerdo de Evaluaciones de Impacto, 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 Órgano Garante Local 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 órgano administrativo respectivo, atenderá las observaciones que en su caso realice el Órgano Garante Local de la materia.

d) Informe de exención

Cuando a juicio de la Unidad de Transparencia, en conjunto con los órganos administrativos del TAPJECH, se puedan comprometer los efectos que se pretenden lograr con la posible puesta en operación o modificación de políticas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales o se trate de situaciones de emergencia o urgencia, no será necesario realizar la evaluación de impacto en la protección de datos personales; lo anterior de conformidad con el artículo 79 de la Ley General de Protección, en adminiculación con el numeral 107 de la Ley Estatal de Protección.

Tratándose del supuesto anterior, durante los primeros 30 días hábiles posteriores a la fecha de la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, la Unidad de Transparencia deberá presentar el informe de exención previsto en el artículo 34 del Acuerdo de Evaluaciones de Impacto; informe que se hará del conocimiento del Comité de Transparencia.

XVI.- Capacitación

Este apartado se refiere a la capacitación que deberá otorgarse a las personas servidoras públicas del TAPJECH en materia de protección de datos personales.

El Comité de Transparencia y la Unidad de Transparencia, se apoyarán en los órganos administrativos para establecer un programa de capacitación y actualización en materia de protección de datos personales, el cual, de conformidad con los artículos 92 de la Ley General de Protección, 123 de la Ley Estatal de Protección, así como 48 y 64 de los Lineamientos Generales de Protección, deberá dirigirse a todos los órganos jurisdiccionales y administrativos del TAPJECH.

XVII.- Revisión y auditoría

Este apartado se refiere a la forma en que deberán ser supervisadas, monitoreadas y revisadas las directrices estipuladas para la protección de los datos personales.

En términos de lo previsto en los artículos 33, fracción VII de la Ley General de Protección, en adminiculación del artículo 47, fracción VII de la Ley Estatal de Protección y 63 de los Lineamientos Generales de Protección, las políticas y directrices planteadas en este sistema de gestión deberán ser supervisadas, monitoreadas y revisadas a través de auditorías y revisiones administrativas, cuestión que será efectuada por la Unidad de Transparencia al implementar Mecanismos de Monitoreo, Revisión, Alertas, Vulneraciones y Auditoría, que disponga el órgano garante local, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, o en su caso, el Comité de Transparencia, bajo las consideraciones que disponga el Pleno del Tribunal.

XVIII.- Procedimiento de orientación y quejas

Este apartado se refiere a los mecanismos disponibles para orientar a las personas titulares en la protección de sus datos personales o recibir las quejas derivadas de su tratamiento.

De conformidad con el artículo 35, fracción VI de la Ley General de Protección, en relación con el numeral 51, fracción XVIII de la Ley Estatal de Protección, entre los mecanismos que deben adoptarse para cumplir con el principio de responsabilidad se encuentra la implementación de un procedimiento para recibir y responder dudas y quejas de los titulares de los datos personales.

El artículo 50 de los Lineamientos Generales de Protección, dispone que tal procedimiento debe tener las características siguientes:

- Ser de fácil acceso y con la mayor cobertura posible.
- Considerar el perfil de los titulares y la forma en que se mantiene contacto o comunicación directa o cotidiana con ellos.
- Estar habilitado en todo momento.

Considerando lo anterior, la Unidad de Transparencia contará con un Procedimiento de Orientación y Quejas a través del cual, las personas titulares de los datos personales se encuentren en oportunidad de recibir la orientación correspondiente a sus cuestionamientos y quejas.

Al respecto, a efecto de extender los alcances del citado procedimiento, se implementará de primera cuenta en modalidad física.

La Unidad de Transparencia, informará a las personas titulares de los datos personales que acudan ante ella, la posibilidad de poder manifestar verbalmente o a través de un escrito, las dudas y quejas que surjan relativo al tratamiento respectivo.

La atención de tales cuestionamientos, corresponderá a la persona que desempeñe la función de Oficial de Protección de Datos Personales adscrita a la Unidad de Transparencia, quien brindará la orientación correspondiente.

Por otro lado, atendiendo a que el trámite del ejercicio de los derechos ARCO se desarrolla a través de los acuerdos internos que emite la Unidad de Transparencia, que son notificados a los solicitantes respectivos, en cada una de tales determinaciones se deberán inscribir los datos de contacto a través de los cuales podrán comunicarse ante dudas, cuestionamientos y quejas.

XIX.- Acciones para la mejora continua

Este apartado se refiere a la forma en que se documentarán las acciones para la mejora continua de la protección de los datos personales en el TAPJECH.

Con la finalidad de que el presente Sistema se mantenga en constante perfeccionamiento, deberán documentarse las acciones para su mejora continua.

En ese sentido, la Unidad de Transparencia, por sí o a petición de los órganos jurisdiccionales y administrativos, dará cuenta al Comité de Transparencia de los puntos de mejora en materia de protección de datos personales que hayan sido advertidos de las auditorías y revisiones realizadas, o bien, que se estimen relevantes o de inmediata aplicación para perfeccionar las directrices incluidas en el sistema.

Por tanto, una vez ejecutados los Mecanismos de Monitoreo, Revisión, Alertas, Vulneraciones y Auditoría, los puntos de mejora que surjan serán sometidos a conocimiento del Comité de Transparencia.

La Unidad de Transparencia, deberá documentar los resultados y revisiones de los puntos de mejora desarrollados.

XX.- Sanciones

Este apartado se refiere a las sanciones aplicables en caso de incumplimiento de las obligaciones en materia de protección de datos personales o de las relativas al trámite del ejercicio de los derechos ARCO.

a) Incumplimiento de las obligaciones en materia de protección de datos personales

De conformidad con el artículo 191 de la Ley Estatal de Protección, las causas de sanción por incumplimiento de las obligaciones establecidas en la Ley General de Protección, y en la Ley Estatal de Protección, serán 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 Estatal de Protección, 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 Estatal de Protección, 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 Estatal de Protección.

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 ya sea simplificado o integral, o bien, omitir en el mismo alguno de los elementos a que refieren los artículos establecidos en la Ley Estatal de Protección, según sea el caso, y demás disposiciones que resulten aplicables en la materia.

IX. Clasificar, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas. 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 57 de la Ley Estatal de Protección.

XI. No establecer las medidas de seguridad en los términos que establecen los artículos 47, 48 y demás aplicables de la Ley Estatal de Protección.

XII. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad.

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

XIV. Obstruir los actos de verificación de la autoridad.

XV. Crear bases de datos personales en contravención a lo dispuesto por el artículo de la Ley Estatal de Protección.

XVI. No acatar las resoluciones emitidas por el Órgano Garante Local.

XVII. Aplicar medidas compensatorias en contravención de los criterios que para tales fines establezca el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

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 Órgano Garante Local.

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 86, 87, 92 y demás aplicables de la Ley Estatal de Protección, respecto a la formalización de la relación responsable y encargado y cómputo en la nube.

XXII. No presentar ante el Órgano Garante Local, 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 Estatal de Protección y demás normativa aplicable.

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

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, entregar el mismo día de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, XV, XVI, XVIII, XIX y XX, del artículo en referencia, 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.

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

b) Incumplimiento por parte de los órganos jurisdiccionales y administrativos, en el ejercicio de los derechos ARCO

Cuando algún órgano jurisdiccional y/o administrativo se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, ésta última dará aviso al superior jerárquico del órgano jurisdiccional y/o administrativo respectivo, para que ordene realizar sin demora las acciones conducentes, conforme al artículo 105 de los Lineamientos Generales de Protección.

Si persiste la negativa de colaboración, la Unidad de Transparencia lo hará del conocimiento del Comité de Transparencia para que, a su vez, dé vista a la Contraloría del TAPJECH y, en su caso, se inicie el procedimiento de responsabilidad administrativa respectivo.

DISPOSICIONES TRANSITORIAS

Primera: El presente Sistema de Gestión de Seguridad en materia de Protección de Datos Personales del Tribunal Administrativo del Poder Judicial del Estado de Chiapas, entrará en vigor al día siguiente de su aprobación, por parte del Pleno del Tribunal.

Segunda: Se deroga cualquier otra disposición que se oponga o contravenga a lo establecido en el presente instrumento.

Tercera: En los casos en que se presente controversia en cuanto a la interpretación, aplicación y observancia del presente Sistema de Gestión de Seguridad, el Comité de Transparencia del Tribunal Administrativo del Poder Judicial del Estado de Chiapas resolverá lo conducente, conforme a los artículos 113 y 114 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

Cuarta: Todos los nombramientos del personal, incluidos aquellos expedidos a partir del inicio en funciones de este Tribunal, estarán sujetos a las disposiciones del inciso 9) “Deber de Confidencialidad”, en el punto VII de los Mecanismos para cumplir con los principios y deberes, establecidas en este ordenamiento.

Quinta: Publíquese el presente Sistema de Gestión de Seguridad en la página electrónica del Tribunal Administrativo del Poder Judicial del Estado de Chiapas.

Dado en el salón del Pleno del Tribunal Administrativo del Poder Judicial del Estado, en la Ciudad de Tuxtla Gutiérrez, Chiapas; a los 05 días del mes de septiembre del año 2023.

Magistrada Presidenta Susana Sarmiento López, Magistrada Mónica de Jesús Trejo Velázquez y Magistrado Víctor Marcelo Ruiz Reyna, ante la fe de la Secretaria General de Acuerdos y del Pleno Fabiola Antón Zorrilla.

SUSANA SARMIENTO LÓPEZ
MAGISTRADA PRESIDENTA

MÓNICA DE JESÚS TREJO VELÁZQUEZ
MAGISTRADA

VÍCTOR MARCELO RUIZ REYNA
MAGISTRADO

FABIOLA ANTÓN ZORRILLA
SECRETARIA GENERAL DE ACUERDOS Y DEL PLENO