



SECRETARÍA
DE EDUCACIÓN
GOBIERNO DE CHIAPAS

SISTEMA DE GESTIÓN DATOS PERSONALES

Unidad de Transparencia

JUNIO 2023

Índice

Introducción	3
Objetivo	4
Glosario	4
Medidas de Seguridad	6
Aspectos Generales para el adecuado tratamiento de datos personales	7
Marco normativo	7
Principios que rigen la protección de datos personales	7
Políticas para la protección de datos personales	7
Deberes que rigen la protección de datos personales	10
Ciclo de vida de los datos personales	10
Prohibición de tratamientos que tengan como efecto cualquier tipo de discriminación	11
Privilegiar el interés superior del niño, niña y adolescente	11
Atribuciones y obligaciones	11

Materialización del cumplimiento de principios y deberes	13
Transferencia de datos personales	24
Remisión de datos personales	27
Cómputo en la nube	29
Ejercicio de Derechos ARCO	31
Portabilidad	32
Ciclo de Vida de los datos personales	32
Procedimiento de Orientación y Quejas	35
Evaluaciones de Impacto	37
Sanciones	41

Introducción

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, establece 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, que será el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en dicha legislación y las disposiciones que resulten aplicables en la materia.

Por su parte los Lineamientos Generales de Protección de Datos Personales para el Sector Público, estipula que el sistema de gestión deberá permitir planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad.

Así mismo, este documento tiene como propósito controlar internamente el universo de datos personales que posee la Secretaría de Educación, el tipo de datos personales que contiene cada unidad administrativa, los responsables, encargados, usuarios de cada tratamiento y las medidas de seguridad concretas implementadas, los análisis de riesgo y brecha, las bitácoras de acceso, vulneraciones, así como el plan de capacitación.

En cumplimiento a lo anterior, la Unidad de Transparencia de la Secretaría de Educación se avocó a la elaboración del presente Sistema de Gestión de Seguridad de Datos Personales, mismo que fue sometido a aprobación del Comité de Transparencia, que es la autoridad máxima en materia de protección de datos personales dentro de este sujeto obligado, contando con la atribución de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales.

Objetivo

4

El presente documento, forma parte de las políticas internas y de gestión del tratamiento de datos personales de la Secretaría, cuyos objetivos son los siguientes:

1. Establecer las acciones que se llevarán a cabo tendientes al establecimiento de medidas de seguridad para el tratamiento de datos personales en la Secretaría.
2. Definir las actividades que llevan a cabo las áreas administrativas para la implementación, monitoreo y buenas prácticas en el tratamiento y seguridad de los datos personales en la Secretaría, lo anterior mediante:
 - ❖ El conocimiento del marco normativo y políticas aplicables en el tratamiento de datos personales.
 - ❖ El establecimiento de la política interna de gestión y tratamiento de datos personales tomando en consideración: Atribuciones y obligaciones de las unidades administrativas; principios y deberes que rigen el tratamiento, transferencia, remisión, uso de cómputo en la nube, el ejercicio de derechos ARCO, derecho de portabilidad, ciclo de vida, supresión, los procedimientos de orientación, atención de quejas, evaluaciones de impacto y sanciones relacionadas con el tratamiento de datos personales.

Glosario

Áreas administrativas: Las áreas de la Secretaría de Educación del estado de Chiapas que cuentan o puedan contar con información que se encuentren previstas en la normativa de la materia.

Comité de Transparencia: El Comité de Transparencia es la autoridad máxima en materia de protección de datos personales el cual se integrará y funcionará conforme a lo dispuesto en la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y demás normativa aplicable.

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

Sistema de Gestión Datos Personales

Datos personales sensibles: Aquellos que se refieren a la esfera más íntima de una persona, por ejemplo, origen racial o étnico, salud, religión, orientación política, preferencia sexual.

Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable, que trata datos personales a nombre y por cuenta de éste.

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

Instituto: Instituto de Transparencia Acceso a la Información y Protección de Datos Personales del Estado de Chiapas

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

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

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

Responsable: Son los sujetos obligados que deciden sobre determinado tratamiento de datos personales, cuestión que implica determinar el tipo de datos personales a tratar, la categoría de titular, las finalidades o usos a que serán sometidos los datos personales, entre otras decisiones.

Unidad: Unidad de Transparencia de la Secretaría de Educación.

Secretaría: Secretaría de Educación del Estado de Chiapas.

Titular: Persona física a quien corresponden los datos personales.

Tratamiento: Operación manual o automatizada aplicada a los datos personales. Sirvan como ejemplo a manera enunciativa más no limitativa: obtención, uso, registro, organización, conservación, difusión, transferencia, entre otros.

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

I. 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. Al respecto, las medidas de seguridad administrativas, físicas y técnicas operadas por las áreas administrativas de la Secretaría, son descritas de manera general en el Documento de Seguridad, el cual incluye los mecanismos que serán operados por la Unidad de Transparencia para su monitoreo, revisión, supervisión y auditoría.

Dentro de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el análisis de riesgo, análisis de brecha y plan de trabajo, forman parte del documento de seguridad de la Secretaría.

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.

II. Aspectos generales para el adecuado tratamiento de datos personales



A. MARCO NORMATIVO

- Constitución Política de los Estados Unidos Mexicanos
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas

B. POLÍTICAS PARA LA PROTECCIÓN DE DATOS PERSONALES

En todo tratamiento de datos personales que se realice en la Secretaría, se deberán respetar los principios y deberes dispuestos en la Ley y de conformidad con lo estipulado en los Lineamientos Generales, considerando el ciclo de vida de los datos personales.

Asimismo, se deberá privilegiar el interés superior del niño, niña y adolescente, quedando prohibidos los tratamientos que tengan como efecto cualquier tipo de discriminación.

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

C. 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.

Sistema de Gestión Datos Personales

- ✓ Implica el deber de identificar en la normatividad aplicable las facultades que autorizan a los responsables a tratar datos personales.

8

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.
- Implica el deber de determinar el uso concreto, lícito, explícito y legítimo que se le va a dar a los datos personales.
- ¿Cambios a las finalidades? Requieren el consentimiento de los titulares. Los responsables podrán tratar los datos personales para finalidades distintas a aquéllas que motivaron el tratamiento de los datos personales cuando cuenten con el consentimiento del titular y con atribuciones conferidas en ley.

Lealtad

- ✓ El 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.
- Implica el deber de no actuar de manera engañosa o fraudulenta: sin dolo, error o mala fe.

Consentimiento

- ✓ Cuando no se actualicen algunas de las causales de excepción, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales.
- Implica el deber de recolectar información personal sólo con la autorización, expresa o tácita, según corresponda, del titular (salvo excepciones).

Sistema de Gestión Datos Personales

Calidad

- ✓ El 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 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.

Proporcionalidad

- ✓ El responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

Información

- ✓ El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

Responsabilidad

- ✓ Implica el deber de implementar políticas, programas y mecanismos obligatorios y exigibles al interior de la organización del responsable que acrediten el cumplimiento de los principios, deberes y obligaciones previstos en la Ley. El responsable está obligado a la rendición de cuentas ante el titular y los organismos garantes, según corresponda.

D. DEBERES QUE RIGEN LA PROTECCIÓN DE DATOS PERSONALES

10

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 la Secretaría 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 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.

E. CICLO DE VIDA DE LOS DATOS PERSONALES

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

1. Obtención.	<ul style="list-style-type: none">• Licitud• Información• Consentimiento• Proporcionalidad• Seguridad• Confidencialidad
2. Uso (registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento divulgación, transferencia o disposición).	<ul style="list-style-type: none">• Calidad• Finalidad• Lealtad• Seguridad• Confidencialidad

Sistema de Gestión Datos Personales

3. Eliminación.	<ul style="list-style-type: none">• Calidad• Seguridad• Confidencialidad
-----------------	--

11

En esta dirección, todas las unidades administrativas deberán alinear cada etapa del ciclo de vida **de acuerdo al principio y deber específico**.

F. 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.

G. PRIVILEGIAR EL INTERÉS SUPERIOR DEL NIÑO, NIÑA Y ADOLESCENTE

Las áreas administrativas que, en ejercicio de sus funciones realicen el tratamiento de datos personales, deberán privilegiar el interés superior del niño, niña y adolescente, 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 y los Lineamientos Generales.

H. ATRIBUCIONES Y OBLIGACIONES

La Ley establece las acciones que deberán llevar a cabo el Comité de Transparencia, la Unidad de Transparencia y las instancias en la protección, tratamiento y conservación de los datos personales.

Sistema de Gestión Datos Personales

Las políticas internas de protección de datos personales son de observancia obligatoria para todos (los servidores públicos) que intervengan en cualquier fase de tratamiento de la Secretaría.

Tales acciones, en esencia, constituyen las atribuciones y obligaciones aquí descritas:

Comité de Transparencia

- Aprobar las políticas y programas internos de protección de datos personales. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales.
- Supervisar el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.
- Dar vista al Órgano de Control Interno en aquellos casos en que tenga conocimiento de una presunta irregularidad respecto de determinado tratamiento de datos personales.

Unidad de Transparencia

- Elaborar las políticas y programas internos de protección de datos personales.
- Establecer un sistema de supervisión de vigilancia para comprobar el cumplimiento de las políticas en materia de datos personales.
- Documentar el Sistema de Gestión de Seguridad y elaborar el documento de seguridad.
- Documentar el plan de trabajo de la Secretaría

Áreas administrativas

- Observar los principios de protección de datos personales.
- Cumplir con los deberes de protección de datos personales.

Sistema de Gestión Datos Personales

- Mantener estricto control sobre los datos personales que obran en sus archivos teniendo prohibida su difusión, uso o acceso no autorizado incluso finalizado el tratamiento.

13

I. MATERIALIZACIÓN DEL CUMPLIMIENTO DE PRINCIPIOS Y DEBERES

1. DEBER DE SEGURIDAD

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

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.

Áreas administrativas responsables:

- Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento:

- Implementar las medidas de seguridad que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o su 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, las áreas administrativas competentes deberán dar aviso a la Unidad de Transparencia, con la finalidad de realizar las modificaciones pertinentes al Documento de Seguridad de la Secretaría.

Sistema de Gestión Datos Personales

- 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.

Medios para acreditar el cumplimiento:

- Evidencia generada por cada instancia respecto de la implementación de las directrices, controles, mecanismos y procedimientos de seguridad previstos en el Documento de Seguridad de la Secretaría.

2. DEBER DE CONFIDENCIALIDAD:

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

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.

Áreas administrativas responsables:

- Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento:

- Implementar controles y medidas de seguridad que garanticen el sigilo y la protección de los datos personales.
- En caso de elaborar un contrato, establecer cláusulas que obliguen a la confidencialidad de los datos personales a los terceros que intervengan en su tratamiento.

Medios para acreditar el cumplimiento:

- Atento a la atribución conferida relativa a operar mecanismos de administración del personal de la Secretaría, dicha Dirección se encontrará obligada de hacer del conocimiento de toda persona a quien se le confiera un cargo, el deber de confidencialidad que debe guardar respecto del tratamiento

Sistema de Gestión Datos Personales

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 del servidor público que, de conformidad con 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 sus relaciones con la Secretaría. Lo anterior, sin menoscabo de lo establecido en las disposiciones de acceso a la información pública. ”

- Controles o mecanismos administrativos, técnicos o físicos que se hayan implementado por cada instancia para proteger los datos personales.

PRINCIPIO DE LICITUD

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

Obligación

la solicitud y recepción de los datos personales para su tratamiento a las atribuciones o facultades previstas en la normatividad del procedimiento Ley y en las demás disposiciones legales que rigen su actuar.

Áreas administrativas responsables:

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

Cumplimiento

- Identificar la disposición normativa que faculta a la instancia 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 a la instancia para llevar a cabo el tratamiento correspondiente.

Medios para acreditar el cumplimiento

- Acreditar que cada tratamiento de datos personales encuentre sustento en las atribuciones o facultades del área administrativa Respectiva.

PRINCIPIO DE LEALTAD

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

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, un trato injusto o arbitrario en su contra.

Áreas administrativas responsables

- ✓ Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento

- Llevar a cabo el tratamiento de los datos personales únicamente para los fines comunicados al titular en el Aviso de Privacidad.
- 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 y Lineamientos Generales.
- Evitar que el tratamiento de los datos personales provoque a su titular discriminación, un trato injusto o arbitrario en su contra.

Sistema de Gestión Datos Personales

Medios para acreditar el cumplimiento:

- En el ámbito de su respectiva competencia, las áreas administrativas deberán atender lo siguiente:
 - La obtención de los datos personales deberá realizarse de manera clara y sencilla, acorde a las atribuciones y facultades de las áreas administrativas para realizar el tratamiento.
 - . Poner a disposición de los titulares el Aviso de Privacidad respectivo, para evidenciar que los datos personales obtenidos se utilizarán conforme a lo señalado en el propio aviso y en la normatividad aplicable.
 - 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.

PRINCIPIO DE INFORMACIÓN

- ✓ Debe observarse preponderantemente en la etapa de obtención de los datos personales, aunque también ocupa en algunas ocasiones la etapa de uso (cambio de finalidad o transferencias)

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.

Áreas administrativas responsables

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

Cumplimiento

18

- Atendiendo al momento y manera en la que se recaban los datos personales, se debe acreditar la puesta a disposición del titular el aviso de privacidad. Para ello, cada Unidad Administrativa deberá identificar el momento y el medio por el que se pondrá a disposición.

Medios para acreditar el cumplimiento:

- Los avisos de privacidad deberán contener las características y elementos previstos en la normatividad correspondiente. Las áreas administrativas deberán verificar que el aviso de privacidad sea puesto a disposición atendiendo la normativa.
- Deberán notificar a la Unidad de Transparencia cualquier cambio en el tratamiento de datos personales que requiera una modificación al aviso de privacidad respectivo.

PRINCIPIO DE CONSENTIMIENTO

- ✓ Debe observarse preponderantemente en la etapa de obtención de los datos personales, aunque también ocupa en algunas ocasiones la etapa de uso (cambio de finalidad o transferencias)

Obligación:

- En caso de no actualizar alguno de los supuestos previstos en el artículo 22 de la Ley General, se deberá obtener el consentimiento libre, específico e informado del titular de los datos personales, de conformidad con lo dispuesto en el artículo 20 de dicha Ley General.
- El consentimiento podrá manifestarse de forma tácita, expresa o expresa por escrito.
- Por regla general será válido el consentimiento tácito, salvo que la Ley General o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente.
- Para contar con el consentimiento tácito del titular de los datos, bastará que habiéndose puesto a su disposición el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

Sistema de Gestión Datos Personales

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

19

Áreas administrativas responsables:

- ✓ Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento:

- Identificar si para realizar el tratamiento de los datos personales es necesario el consentimiento de su titular, o si se encuentra dentro de las excepciones previstas en la Ley General.
- En caso de que sea necesario recabar el consentimiento del titular, definir el tipo de consentimiento que resulta aplicable
- De acuerdo con la forma en que los datos personales son obtenidos (directa o indirectamente del titular), establecer la forma y el momento en que debe obtenerse el consentimiento.
- En caso de que 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.

Medios para acreditar el cumplimiento:

- Las áreas administrativas que conforme a sus atribuciones hayan emitido un Aviso de Privacidad, deberán mantener el registro de su publicación, difusión y puesta a disposición.
- Las áreas administrativas que obtengan o reciban datos personales que se ubiquen en el supuesto de un consentimiento expreso, deberán documentar su obtención.

PRINCIPIO DE PROPORCIONALIDAD

- ✓ Debe observarse en la etapa de obtención de los datos personales

Sistema de Gestión Datos Personales

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 instancia 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.

Áreas administrativas responsables:

- Todas aquellas que realicen el tratamiento de datos personales.
- Las áreas administrativas que, en ejercicio de sus funciones realicen el tratamiento de datos personales, deberán privilegiar el interés superior del niño, niña y adolescente, 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 y los Lineamientos Generales.

Medios para acreditar el cumplimiento:

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

PRINCIPIO DE FINALIDAD

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

Obligación:

- Todo tratamiento de datos personales debe estar justificado en razón de finalidades concretas, lícitas, explícitas y legítimas.

Sistema de Gestión Datos Personales

- En todo momento, las finalidades deben estar relacionadas con las atribuciones normativas de la instancia 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 la instancia respectiva cuente con:
 1. Atribuciones legales para ello.
 2. En caso de que la finalidad no actualice alguno de los supuestos de excepción, contar con el consentimiento del 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 titular, basada en la relación que la instancia mantiene con éste.
- La naturaleza de los datos personales.
- Las consecuencias para 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 y Lineamientos Generales.

Áreas administrativas responsables:

Todas aquellas que realicen el tratamiento de datos personales.

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

Sistema de Gestión Datos Personales

de manera clara, de manera que el consentimiento del 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 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, solicitar el consentimiento de los titulares para el tratamiento de las finalidades adicionales, en términos de las reglas para el consentimiento para el tratamiento de datos personales.

Medios para acreditar el cumplimiento:

- 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, el área administrativa 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, la instancia 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.

PRINCIPIO DE CALIDAD

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

Obligación:

- Las áreas administrativas 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 área administrativa.
- 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.

Áreas administrativas responsables:

- Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento:

Para acreditar el cumplimiento del principio de calidad, las áreas administrativas 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.

Medios para acreditar el cumplimiento:

- En todo momento, las áreas administrativas 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, las áreas administrativas deberán conservar las constancias o anotaciones respectivas.

J. TRANSFERENCIA DE DATOS PERSONALES

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

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

- ✓ Su titular.
- ✓ La Secretaría.
- ✓ Los encargados contratados por la Secretaría.

De los artículos 65 y 66 de la Ley General se desprenden dos reglas aplicables a las transferencias de datos personales:

1. Toda transferencia de datos personales sea nacional o internacional, se encuentra sujeta a consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de la Ley General.
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 a la Secretaría, con excepción de los supuestos previstos en el artículo 66 de la Ley General.

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.

Sistema de Gestión Datos Personales

Lo anterior implica que, las áreas administrativas deben contar con el consentimiento del titular de los datos personales para realizar transferencias. Con excepción de los supuestos siguientes:

25

- I. Cuando la transferencia esté prevista en la Ley General u otras leyes, convenios o tratados internacionales suscritos y ratificados por México.
- II. Cuando la transferencia se realice entre la Secretaría 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.
- III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia.
- IV. 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.
- V. 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.
- VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre la Secretaría y el titular de los datos personales.
- VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por la Secretaría y un tercero.
- VIII. Cuando se trate de los casos en los que la Secretaría no está obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales.
- IX. 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**, las áreas administrativas deberán realizar las gestiones necesarias para recabarlo.

Sistema de Gestión Datos Personales

Al respecto, por regla general el consentimiento a que se refiere el punto anterior será **tácito**, salvo que una ley exija a la Secretaría recabar el consentimiento expreso para la transferencia de sus datos personales.

Cuando se requiera el consentimiento expreso, la instancia podrá establecer cualquier medio lícito que le permita obtenerlo de manera previa a la transferencia de los datos personales.

En todos los casos, las áreas administrativas deberán verificar que en el **aviso de privacidad** correspondiente al tratamiento en que los datos personales fueron recabados, se realice lo siguiente:

1.-Se informe al titular de la transferencia a realizar.

Los mecanismos y medios disponibles para que 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.

2.-La Secretaría 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.

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.

Sistema de Gestión Datos Personales

- 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.

27

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, las áreas administrativas 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 y las disposiciones que resulten aplicables en la materia.

K. REMISIÓN DE DATOS PERSONALES

Este apartado se refiere a los aspectos que las áreas administrativas deberán observar al efectuar una remisión de datos personales.

La remisión se refiere a toda comunicación de datos personales realizada exclusivamente entre la Secretaría y una persona ajena que sola o conjuntamente con otras, efectuará el tratamiento de datos personales a nombre y por cuenta de la propia Secretaría.

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

Sistema de Gestión Datos Personales

Las áreas administrativas 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 de la Secretaría 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 de la Secretaría o de lo instruido en el contrato o instrumento jurídico respectivo.
- ✓ Implementar medidas de seguridad conforme a la Ley General, Ley Estatal, Lineamientos Generales y los instrumentos jurídicos aplicables.
- ✓ Informar inmediatamente sobre la vulneración de datos personales a la instancia de la Secretaría con quien se haya realizado la remisión de estos.
- ✓ Durante y después de la transferencia 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 la Secretaría, 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 la Secretaría 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 la Secretaría o con el Instituto, 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 todas las áreas administrativas 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

Sistema de Gestión Datos Personales

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.

Cuando el encargado incumpla las instrucciones de la Secretaría 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.

Subcontrataciones en 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, las áreas administrativas 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 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.

L. CÓMPUTO EN LA NUBE

Este apartado se refiere a los aspectos que las áreas administrativas deberán observar al contratar servicios de cómputo en la nube.

Sistema de Gestión Datos Personales

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.

Las áreas administrativas de la Secretaría 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 que resulten aplicables en la materia.

En caso de que la Secretaría 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 la Secretaría 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:

1. Contar con políticas de protección de datos personales de conformidad con la normativa aplicable.
2. Dar cuenta de las subcontrataciones que involucren información sobre la que se presta el servicio.
3. Abstenerse de asumir la titularidad o propiedad de la información sobre la que se preste el servicio.
4. Guardar confidencialidad de los datos personales que se traten.
5. Contar con medidas de seguridad para la protección de datos personales.
6. Garantizar la supresión de los datos personales una vez finalizada la relación jurídica.
7. Impedir el acceso no autorizado a los datos personales sujetos a tratamiento.

Sistema de Gestión Datos Personales

Es importante referir que, de conformidad con lo estipulado en el artículo 111 de los Lineamientos Generales, los proveedores de servicios de cómputo en la nube tendrán el carácter de encargados, por lo que la instancia que pretenda contratar sus servicios deberá verificar el cumplimiento de lo estipulado en el capítulo de este programa denominado “Remisión de datos personales”; es decir, además de observar las obligaciones señaladas, deberá incluir en el contrato o instrumento jurídico las obligaciones generales establecidas en la normativa de la materia.

31

M. EJERCICIO DE DERECHOS ARCO

Los titulares cuentan con los derechos siguientes:

- **Acceder** a sus datos personales, así como a conocer la información relacionada con las condiciones y generalidades de su tratamiento.
- **Rectificar** sus datos personales. El titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.
- **Cancelar** sus datos personales. El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.
- **Oponerse** al tratamiento de sus datos personales. El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando:
 - Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular.
 - Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular su rendimiento profesional, situación

Sistema de Gestión Datos Personales

económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

32

N. PORTABILIDAD

Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos 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.

El trámite a las solicitudes de ejercicio de los referidos derechos, será substanciado por la Unidad de Transparencia, en términos del Procedimiento establecido.

O. CICLO DE VIDA DE LOS DATOS PERSONALES

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, 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,

Sistema de Gestión Datos Personales

- Divulgación,
- Retención y
- Destrucción.

33

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

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 se prevea 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.

Cada instancia 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.

P. SUPRESIÓN DE DATOS PERSONALES

34

Es la eliminación de los datos personales Cuando éstos hayan logrado cumplir con su objetivo y entonces puedan finalizar su ciclo de vida.

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 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, seguridad y confidencialidad, favorable al medio ambiente.

En este orden de ideas, las áreas administrativas para suprimir los datos personales deberán:

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

Q. PROCEDIMIENTO DE ORIENTACIÓN Y QUEJAS

35

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.

Este 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, se establece el siguiente procedimiento:

- El Titular de Datos Personales envía la Solicitud de Queja o Aclaración con la documentación adjunta a la Unidad de Transparencia.

La Solicitud de Queja o Aclaración, deberá contar con la siguiente información:

1. Nombre(s), Primer Apellido, Segundo Apellido y Domicilio actual o Domicilio para oír y recibir notificaciones.
2. Número Telefónico y/o Correo Electrónico donde se le pueda localizar.
- 3.-Acreditarse debidamente mediante documento idóneo.
4. Descripción precisa y clara de los hechos en los que considere que se haya vulnerado sus Datos Personales.

Recibida la solicitud o queja, el área administrativa contará con 5 días para verificar que la solicitud sea clara, correcta y precisa.

Cuando la solicitud no sea clara, precisa o tenga información errónea o incompleta, se solicita al Titular de los Datos Personales que aporte información adicional para atender su petición. Esta solicitud se debe realizar dentro de los 5 días hábiles siguientes a la recepción de la Solicitud.

Sistema de Gestión Datos Personales

El Titular de Datos Personales contará con 10 días hábiles para atender el requerimiento de información adicional, contados a partir del día siguiente en que lo haya recibido, de no recibir respuesta del Titular de Datos Personales, la solicitud se tendrá por no presentada.

En caso de que Titular de Datos Personales atienda el requerimiento de información, el plazo para que se dé respuesta a la solicitud, empezará a correr al día siguiente de que el Titular de Datos Personales envíe el requerimiento correcto y completo.

El responsable de los Datos Personales, analiza la solicitud para comunicar al Titular de Datos Personales si procede la solicitud o se informa la negativa.

Si se trata de una queja, se verifica si existe vulneración de Derechos.

Si existe vulneración de derechos, se tomarán medidas para que la falta no se siga presentando, iniciando un proceso administrativo interno para aplicar las sanciones que correspondan; notificando al área donde se está generando la vulneración.

Si no existe una vulneración de derechos, se documentarán las pruebas pertinentes para notificar al solicitante.

Si se trata de una aclaración, se documentará de manera clara y precisa el Tema objeto de aclaración, adjuntando las pruebas pertinentes en caso de aplicar para ser notificadas al Solicitante.

El responsable de los Datos Personales, responderá a la solicitud de queja o aclaración y los motivos de su decisión por el mismo medio que se presentó la solicitud en un plazo máximo de 15 días hábiles contados desde el día en que se haya recibido su Solicitud, acompañando, en su caso, de las pruebas que resulten pertinentes.

La Unidad de Transparencia, notifica al Titular de Datos Personales (utilizando los datos de contacto proporcionados en la Solicitud) la Resolución de la Solicitud de Queja o Aclaración en un plazo no mayor a 15 días hábiles después de dar por recibida la Solicitud

Cuando alguna unidad administrativa se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, ésta deberá dar aviso al superior jerárquico de dicha unidad administrativa, para que le ordene realizar sin demora las acciones conducentes.

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 interna y en su caso, se dé inicio el procedimiento de responsabilidad administrativo respectivo.

R. EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES

Este apartado se refiere a los aspectos que las instancias 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 Instituto.

a) Aspectos generales.

En términos de lo estipulado en el artículo 74 de la Ley General, 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 Instituto, 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 los artículos 75 y 76 de la Ley General y 8 de los Lineamientos para la Evaluación de Impacto, se estará en presencia de un tratamiento intensivo o relevante de datos personales cuando ocurra alguna de las condiciones siguientes:

- 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

Sistema de Gestión Datos Personales

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.

- Se traten datos personales sensibles, 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 más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y orientación sexual.

- Se efectúen o pretendan efectuar transferencias de datos personales, 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.

De acuerdo con lo estipulado en el artículo 9 de los Lineamientos para la Evaluación de Impacto, se entenderá, de manera enunciativa más no limitativa, que se está ante la presencia de un tratamiento intensivo o relevante de datos personales, de manera particular, cuando se pretenda:

- Cambiar la o las finalidades que justificaron el origen de determinado tratamiento de datos personales, de tal manera que pudiera presentarse una incompatibilidad entre las finalidades de origen con las nuevas finalidades, al ser estas últimas más intrusivas para los titulares.

- Evaluar, monitorear, predecir, describir, clasificar o categorizar la conducta o aspectos análogos de los titulares, a través de la elaboración de perfiles determinados para cualquier finalidad, destinados a producir efectos jurídicos que los vinculen o

Sistema de Gestión Datos Personales

afecten de manera significativa, especialmente cuando a partir de dicho tratamiento se establezcan o pudieran establecerse diferencias de trato o un trato discriminatorio económico, social, político, racial, sexual o de cualquier otro tipo que pudiera afectar la dignidad o integridad personal de los titulares.

- Tratar datos personales de grupos vulnerables atendiendo, de manera enunciativa mas no limitativa, a su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica.

- Crear bases de datos concernientes a un número elevado de titulares, aun cuando dichas bases no estén sujetas a criterios determinados en cuanto a su creación o estructura, de tal manera que se produzca la acumulación no intencional de una gran cantidad de datos personales respecto de los mismos.

- Incluir o agregar nuevas categorías de datos personales a las bases de datos ya existentes y en posesión del responsable, de tal forma que, en caso de presentarse una vulneración de seguridad por la cantidad de información contenida en ellas, pudiera derivarse una afectación a la esfera personal de los titulares, sus derechos o libertades.

- Realizar un tratamiento frecuente y continuo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas.

- Utilizar tecnologías con sistemas de vigilancia; aeronaves o aparatos no tripulados; minería de datos; biometría; Internet de las cosas; geolocalización; técnicas analíticas; radiofrecuencia o cualquier otra que pueda desarrollarse en el futuro y que implique un tratamiento de datos personales a gran escala.

- Permitir el acceso de terceros a una gran cantidad de datos personales que anteriormente no tenían acceso, ya sea, entregándolos, recibéndolos y/o poniéndolos a su disposición en cualquier forma.

- Realizar transferencias internacionales de datos personales a países que no cuenten en su derecho interno con garantías suficientes y equivalentes para

Sistema de Gestión Datos Personales

asegurar la debida protección de los datos personales, conforme al sistema jurídico mexicano en la materia.

40

- Revertir la disociación de datos personales para la consecución de finalidades determinadas, especialmente si éstas son de carácter intrusivo o invasivo al titular.
- Tratar datos personales sensibles con la finalidad de efectuar un tratamiento sistemático y masivo de los mismos.
- Realizar una evaluación sistemática y exhaustiva de aspectos propios de las personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para éstas o que les afecten significativamente de modo similar.
- Realizar un tratamiento a gran escala de datos personales sensibles o datos personales relativos a condenas e infracciones penales.
- La observación sistemática a gran escala de una zona de acceso público.

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, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

Las unidades administrativas 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.

Sistema de Gestión Datos Personales

- ✓ 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 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 y los Lineamientos para la Evaluación 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 Instituto con un mínimo de 30 días hábiles previos a la fecha en que se pretenda poner en operación o modificar el tratamiento respectivo.
- ✓ La Unidad de Transparencia, en coordinación con el área administrativa respectiva, atenderá las observaciones que en su caso realice el Instituto.

41

S. 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 163 de la Ley General, serán causas de sanción por incumplimiento de las obligaciones establecidas en la Ley General, las siguientes:

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

Sistema de Gestión Datos Personales

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

III. 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.

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la Ley General.

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la Ley 72 General, según sea el caso, y demás disposiciones que resulten aplicables en la materia.

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales.

VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la Ley General.

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la Ley General.

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la Ley General.

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la Ley General. XI. Obstruir los actos de verificación del INAI.

XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la Ley General.

Sistema de Gestión Datos Personales

XIII. No acatar las resoluciones emitidas por el INAI.

XIV. Omitir la entrega del informe anual y demás informes 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 de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves.

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

b) Incumplimiento por parte de las instancias en el ejercicio de los derechos ARCO

De conformidad con el artículo 105 de los Lineamientos Generales, cuando alguna unidad administrativa se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, ésta deberá dar aviso al superior jerárquico de dicha unidad administrativa, para que le ordene realizar sin demora las acciones conducentes.

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 Poder Judicial de la Federación y, en su caso, se dé inicio el procedimiento de responsabilidad administrativo respectivo.