Consejo de la Judicatura Federal

Sistema de Gestión de Seguridad de Datos Personales

Comité de Transparencia

Consejo de la Judicatura Federal

Índice

Presentación

El artículo 34 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 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*.

Un *sistema de gestión*, es 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.

El artículo 65 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público,[1] 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.

Al respecto, el artículo 15 del Acuerdo General del Pleno del Consejo de la Judicatura Federal que establece las disposiciones en materia de protección de datos personales, determina que la Unidad de Transparencia documentará el sistema de gestión.

En cumplimiento a lo anterior, la Unidad de Transparencia se avocó a la elaboración del presente **Sistema de Gestión de Seguridad de Datos Personales**, mismo que fue sometido a aprobación del Comité de

[1] Publicados en el Diario Oficial de la Federación el 26 de enero de 2018, consultables a través de la liga: http://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018

Transparencia, quien de conformidad con el artículo 83, segundo párrafo y 84, fracción I, de la Ley General, es 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.

Abreviaturas y denominaciones

Acuerdo de Archivo Administrativo: Acuerdo General del Pleno del Consejo de la Judicatura Federal, que establece la organización y conservación de los archivos administrativos del propio Consejo, publicado en el Diario Oficial de la Federación el 20 de marzo de 2020.

Acuerdo de Archivo Jurisdiccional: Acuerdo General del Pleno del Consejo de la Judicatura Federal, que establece las disposiciones en materia de valoración, depuración, destrucción, digitalización, transferencia y resguardo de los expedientes judiciales generados por los órganos jurisdiccionales, publicado en el Diario Oficial de la Federación el 25 de marzo de 2020.

Acuerdo General: Acuerdo General del Pleno del Consejo de la Judicatura Federal que establece las disposiciones en materia de protección de datos personales, publicado en el Diario Oficial de la Federación el 10 de octubre de 2018.

Áreas administrativas: Las unidades administrativas y órganos auxiliares del Consejo de la Judicatura Federal.

CJF: Consejo de la Judicatura Federal.

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

Instancias: Órganos jurisdiccionales y áreas administrativas que en ejercicio de sus atribuciones realicen el tratamiento de datos personales.

Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017.

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Publico, publicados en el Diario Oficial de la Federación el 26 enero de 2018.

Lineamientos para la Evaluación de Impacto: 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, publicados en el Diario Oficial de la Federación el 23 de enero de 2018.

Lineamientos para la Portabilidad: Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, publicado en el Diario Oficial de la Federación el 12 de febrero de 2018.

Objetivo

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

1. Establecer las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales en el CJF.
   - Lo anterior, será desarrollado en el capítulo relativo a las *Medidas de Seguridad.*

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 CJF.
   - Para ello, se puntualizará el marco normativo aplicables y las políticas generales y específicas que deberán regir en el tratamiento de los datos personales.
   - Asimismo, se integrará a este documento un *Programa de Datos Personales* el cual desarrollará los aspectos siguientes:
     - ✓ Las atribuciones y obligaciones de las instancias 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 una transferencia de datos personales.
     - ✓ Las actuaciones que deben ser consideradas al realizar una 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 CJF.
- ✓ Las cuestiones relacionadas con la supresión de datos personales.
- ✓ Las cuestiones relacionadas con las Evaluaciones de Impacto ante el INAI.
- ✓ Las cuestiones relacionadas con la capacitación e materia de protección de datos personales.
- ✓ Las cuestiones relacionadas a la revisión y auditoría de las medidas de seguridad de los datos personales.
- ✓ El establecimiento de un procedimiento de orientación quejas relacionadas con el tratamiento de datos personales.
- ✓ Acciones para la mejora continua.
- ✓ Sanciones aplicables.

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 y 65 de los Lineamientos Generales.

Al respecto, las medidas de seguridad administrativas, físicas y técnicas operadas por las instancias del CJF son descritas de manera general en el *Documento de Seguridad* (**anexo I**), el cual incluye los mecanismos que serán operados por la Unidad de Transparencia 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.

Marco normativo

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

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

- Última reforma al apartado y párrafo publicadas en el Diario Oficial de la Federación el 29 de enero de 2016 y 01 de enero de 2009, respectivamente.

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

- Publicada en el Diario Oficial de la Federación el 26 de enero de 2017.

Lineamientos Generales de Protección de Datos Personales para el Sector Público

- Publicados en el Diario Oficial de la Federación el 26 de enero de 2018.

Acuerdo General del Pleno del Consejo de la Judicatura Federal que establece las disposiciones en materia de protección de datos personales

- Publicado en el Diario Oficial de la Federación el 10 de octubre de 2018.

Políticas para la protección de datos personales

En todo tratamiento de datos personales que se realice en el CJF, se deberán respetar los principios y deberes dispuestos en la Ley General, de conformidad con lo estipulado para ello en los Lineamientos Generales y el Acuerdo General, considerando el ciclo de vida de los datos personales[2].

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.

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

- El responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la

[2] Véase capítulo denominado *Ciclo de vida de los Datos Personales* del Programa de Datos Personales del presente documento.

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, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los 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

- El 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.

b) Deberes que rigen la protección de los datos personales

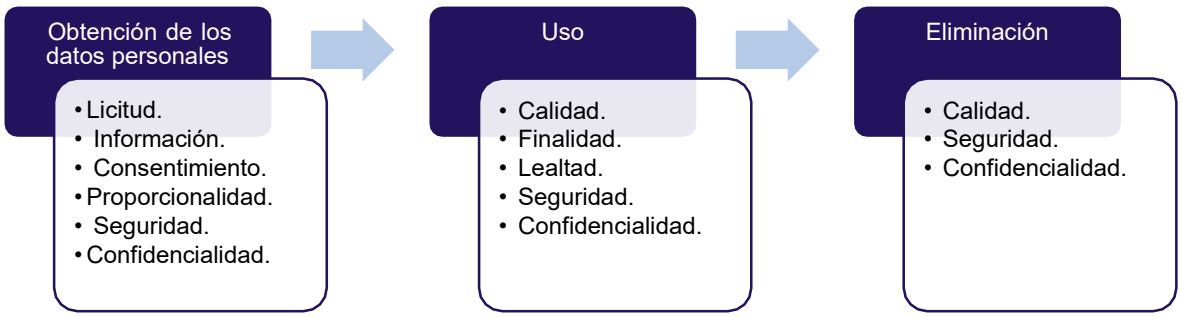
Los deberes que aplican y que se deben observar para el tratamiento de los datos personales son el de **seguridad** y el de **confidencialidad**; el primero, implica que el CJF debe establecer y mantener medidas de carácter administrativo, físico y técnico para la protección de los datos personales en 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.

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

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, las instancias 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 del niño, niña y adolescente.

Las instancias 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.

Programa General de Datos Personales

Atribuciones y obligaciones de las instancias

A través del Acuerdo General, el Pleno del CJF estableció 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**.

Tales acciones, en esencia, constituyen las atribuciones y obligaciones siguientes:

Comité de Transparencia

- Aprobar las 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 a la Contraloría del Poder Judicial de la Federación 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 del CJF.

Instancias

- Observar los principios de calidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad y responsabilidad.
- Adoptar las medidas necesarias para mantener exactos, completos, pertinentes, correctos y actualizados los datos personales en su posesión.
- 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.

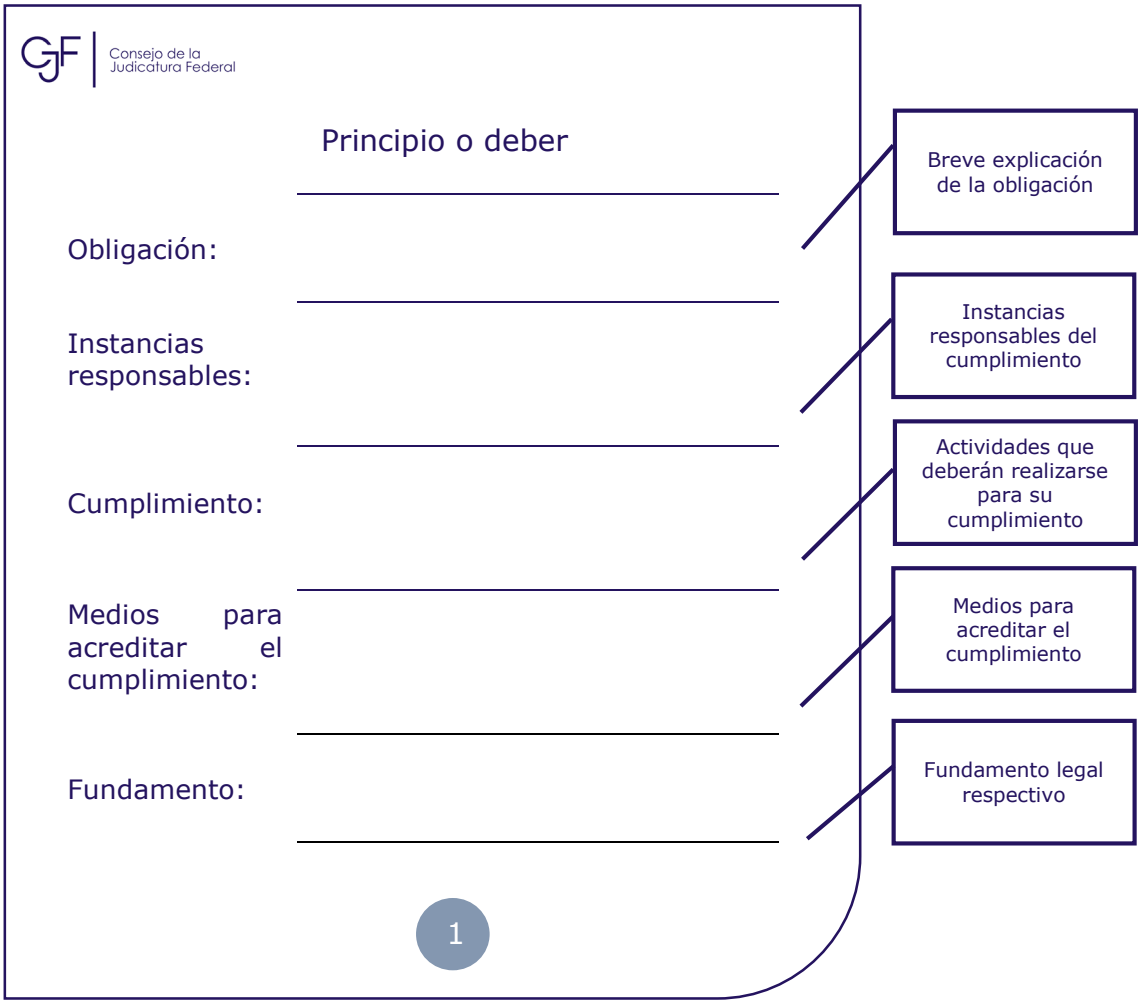
Considerando lo anterior, y con la finalidad de alcanzar los objetivos planteados en el Sistema de Gestión, las políticas y directrices internas de protección de datos personales **resultan de observancia obligatoria para todos los servidores públicos del Consejo de la Judicatura Federal que realicen el tratamiento de datos personales.**

Visión general de los principios y deberes

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

- ✓ Breve explicación de la obligación (principio o deber).
- ✓ Instancias responsables del cumplimiento.
- ✓ Actividades que deberán realizarse para su cumplimiento.
- ✓ Medios para acreditar el cumplimiento.
- ✓ Fundamento legal respectivo.

Tales aspectos, serán representados de la forma que se muestra a continuación:



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.
Instancias 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 instancias competentes deberán dar aviso a la Unidad de Transparencia, con la finalidad de realizar las modificaciones pertinentes al Documento de Seguridad del Consejo de la Judicatura Federal. 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 del Consejo de la Judicatura Federal.
Fundamento:	Artículos 31, 32, 33, 34, 35 y 36 de la Ley General y 55 al 65 de los Lineamientos Generales.

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.

Instancias responsables:

Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento:

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

Medios para acreditar el cumplimiento:

- Atento a la atribución conferida a la Dirección General de Recursos Humanos, relativa a operar mecanismos de administración del personal del Poder Judicial de la Federación, 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 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 el artículo 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 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 el Consejo de la Judicatura Federal.
  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.

Fundamento:

Artículo 42 de la Ley General y 71 de los Lineamientos Generales.

Principio de Licitud

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

Obligación:	Sujetar la solicitud y recepción de los datos personales para su tratamiento a las atribuciones o facultades previstas en la Ley Orgánica del Poder Judicial de la Federación, en los Acuerdos Generales del Consejo de la Judicatura Federal y en las demás disposiciones legales que rigen su actuar.
Instancias 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 de la instancia respectiva.
Fundamento:	Artículo 17 de la Ley General, 8 de los Lineamientos Generales y 14, fracción IV del Acuerdo General.

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.

Instancias responsables:

Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento:

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

Medios para acreditar el cumplimiento:

En el ámbito de su respectiva competencia, las instancias deberán atender lo siguiente:

- La obtención de los datos personales deberá realizarse de manera clara y sencilla, acorde a las atribuciones y facultades de la instancia para realizar el tratamiento.
- Poner a disposición de los titulares el Aviso de Privacidad respectivo, para evidenciar que los datos personales obtenidos se utilizarán conforme a lo señalado en el propio aviso y en la normatividad aplicable.
- 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.

Fundamento:

Artículo 19 de la Ley General y 11 de los Lineamientos Generales.

Principio de Información

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

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.

Instancias responsables:

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

Cumplimiento:

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

Medios para acreditar el cumplimiento:

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

Las instancias competentes deberán verificar que el aviso de privacidad se encuentre:

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

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:

- La instancia cambie su identidad.
- 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.

	• La instancia cambie las finalidades señaladas en el aviso de privacidad original. • Se modifiquen las condiciones de las transferencias de datos personales o se pretendan realizar transferencias no previstas inicialmente y el consentimiento del titular sea necesario.
Fundamento:	Artículos 3, fracción II, 26, 27, 28 y 29 de la Ley General y 26 a 45 de los Lineamientos Generales.

Principio de Consentimiento

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

Obligación:

Para estar en oportunidad de obtener los datos personales y con ello, realizar su tratamiento, **resulta necesario que la instancia cuente con el consentimiento del titular**, salvo que se actualice alguno de los supuestos previstos en el artículo 22 de la Ley General.

Esto es, en caso de **no actualizar** alguno de los supuestos previstos en el artículo 22 de la Ley General, se deberá obtener el consentimiento libre, especifico 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 o expresa.

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.

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.

Instancias responsables:

Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento:

1. 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.
2. En caso de que sea necesario recabar el consentimiento del titular, definir el tipo de consentimiento que resulta aplicable (tácito o expreso).
3. 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.
4. 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.

Para lo anterior, podrá consultarse el *Procedimiento de solicitud de consentimiento para el tratamiento de los datos personales*, que constituye el **anexo II**.

Medios para acreditar el cumplimiento:	• Las instancias que conforme a sus atribuciones hayan emitido un Aviso de Privacidad, deberán mantener el registro de su publicación, difusión y puesta a disposición. • Las instancias que obtengan o reciban datos personales que se ubiquen en el supuesto de un **consentimiento expreso**, deberán documentar su obtención.
Fundamento:	Artículos 20, 21 y 22 de la Ley General y 12 al 20 de los Lineamientos Generales.

Principio de Proporcionalidad

Debe observarse en la etapa de **obtención** de los 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.
Instancias responsables:	Todas aquellas que realicen el tratamiento de datos personales.
Cumplimiento:	Cada instancia 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 instancia deberá requerir el mínimo posible de datos personales para lograr las finalidades para las cuales se obtuvieron.
Medios para acreditar el cumplimiento:	Los datos personales tratados deberán ser adecuados, relevantes y necesarios para ejercer la facultad o atribución que le permite a la instancia realizar el tratamiento respectivo.
Fundamento:	Artículo 25 de la Ley General y 24 y 25 de los Lineamientos Generales.

Principio de Finalidad

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

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 el titular.
- **Lícitas:** cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del 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 titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General.

En todo momento, las finalidades deben estar relacionadas con las atribuciones normativas de la instancia que realice el tratamiento.

Obligación:

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 del artículo 22 de la Ley General, 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 General, Acuerdo General y Lineamientos Generales.

Instancias 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 del Consejo de la Judicatura Federal. En todo momento deberá encontrarse identificado el marco normativo que otorga a las instancias 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 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**, de conformidad con lo establecido en el artículo 44, fracción III de los Lineamientos Generales 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, solicitar el consentimiento de los titulares para el tratamiento de las finalidades adicionales, en términos de las reglas descritas en el *Procedimiento de solicitud de consentimiento para el tratamiento de datos personales*, que constituye el **anexo II** de este documento.
Medios para acreditar el cumplimiento:	Las instancias 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, la instancia 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.
Fundamento:	Artículo 18 de la Ley General y, 9, 10 y 44, fracción III, de los Lineamientos Generales.

Principio de Calidad

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

Obligación:

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

Se 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 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.

Instancias responsables:

Todas aquellas que realicen el tratamiento de datos personales.

Cumplimiento:

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

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 instancias 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 instancias deberán conservar las constancias o anotaciones respectivas.

Fundamento:	Artículos 23 y 24 de la Ley General, y 21 y 22 de los Lineamientos Generales.

Transferencia de datos personales

Este apartado se refiere a los aspectos que las instancias deberán observar al efectuar una transferencia de datos personales[3].

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 CJF.
- Los encargados contratados por el CJF[4].

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 al 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 al CJF, con excepción de los supuestos previstos en el artículo 66 de la Ley General.

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

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

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.

Lo anterior implica que, las instancias 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 u otras leyes, convenios o tratados internacionales suscritos y ratificados por México.
- Cuando la transferencia se realice entre el CJF 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 CJF 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 CJF y un tercero.
- Cuando se trate de los casos en los que el CJF 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.
- 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 instancias deberán realizar las gestiones necesarias para recabarlo.

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

En términos de lo previsto en el artículo 114 de los citados Lineamientos, 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 ese contexto, el consentimiento podrá ser recabado de conformidad con lo establecido para esos efectos en el *Procedimiento de solicitud de consentimiento para el tratamiento de datos personales*, que constituye el **anexo II** de este documento.

En todos los casos, las instancias 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.
- 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, de conformidad con el artículo 27, fracción IV, de la Ley General.

En términos del artículo 113 de los Lineamientos Generales, el CJF 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, 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, las instancias 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.

Respecto del punto anterior, es importante considerar que en términos del artículo 116 de los Lineamientos Generales, el CJF 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, las instancias podrán solicitar a través de la Unidad de Transparencia la gestión ante el INAI de una opinión respecto de la logística de la realización de aquellas transferencias internacionales de datos personales que se pretenda efectuar; por lo que deberá de cumplirse con el procedimiento estipulado en el artículo 117 de los Lineamientos Generales.

Fundamento: Artículos 65 a 71 de la Ley General y 113 a 118 de los Lineamientos Generales.

Remisión de datos personales

Este apartado se refiere a los aspectos que las instancias deberán observar al efectuar una *remisión de datos personales*[5].

A) Aspectos Generales

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

Para efectos de la remisión de datos personales, la persona ajena que sola o conjuntamente con otras efectúe el tratamiento, se le denomina *encargado*[6].

Al respecto, de conformidad con los artículos 59 a 62 de la Ley General y 108 a 110 de los Lineamientos Generales, las instancias 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:

[5] **Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.
[6] **Encargado:** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

- Realizar el tratamiento de los datos personales conforme a la normativa del CJF 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 CJF o de lo instruido en el contrato o instrumento jurídico respectivo.
- Implementar medidas de seguridad conforme a la Ley General, Lineamientos Generales, Acuerdo General y los instrumentos jurídicos aplicables.
- Informar inmediatamente sobre la vulneración de datos personales a la instancia del CJF 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 Consejo de la Judicatura Federal, 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 CJF 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 CJF o con el INAI, 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 instancias 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, cuando el encargado incumpla las instrucciones del CJF 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.

- **Regulación de 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 instancias 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 CJF 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.

Cómputo en la nube

Este apartado se refiere a los aspectos que las instancias deberán observar al contratar servicios de cómputo en la nube[7].

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, las instancias del CJF 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, los Lineamientos Generales, el Acuerdo General y demás disposiciones que resulten aplicables en la materia.

En caso de que el CJF 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 CJF 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:

[7] **Cómputo en la nube:** Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

- Tener y aplicar políticas de protección de datos personales afines a los principios y deberes que establecen la Ley General, los Lineamientos Generales, el Acuerdo General 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:

- Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta.
- Permitir al CJF limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio.
- Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio.
- Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al CJF y que este último haya podido recuperarlos.
- 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 CJF.

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

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 de cualquier encargado, las cuales son:

- Realizar el tratamiento de los datos personales conforme a la normativa del CJF 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 CJF y de lo instruido en el contrato o instrumento jurídico respectivo.
- Implementar medidas de seguridad conforme a la Ley General, Lineamientos Generales, Acuerdo General y los instrumentos jurídicos aplicables.
- Informar a la instancia del CJF 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 Consejo de la Judicatura

Federal, 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 CJF así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
- Permitir y colaborar con el CJF o con el INAI, 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.

Ejercicio de los derechos ARCO

Este apartado se refiere a los aspectos que las instancias deberán considerar ante el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de datos personales[8].

De conformidad con los artículos 43 al 56, 85, fracción II, y 86 de la Ley General y 73 al 107 de los Lineamientos Generales, los titulares cuentan con los derechos siguientes:

- Acceso: es el derecho que tiene el titular de solicitar el acceso a sus datos personales que están en las bases de datos, sistemas, archivos, registros o expedientes del responsable que los posee, almacena o utiliza, así como de conocer información relacionada con el uso que se da a los datos personales.
- Rectificación: es el derecho que tiene el titular de solicitar la rectificación o corrección de sus datos personales, cuando éstos sean inexactos o incompletos o no se encuentren actualizados. En ese sentido, puede solicitar a quien posea o utilice sus datos personales que los corrija cuando los mismos sean incorrectos, estén desactualizados o inexactos.
- Cancelación: es el derecho que tiene el titular de solicitar que sus datos personales se eliminen de los archivos, registros, expedientes, sistemas, bases de datos del responsable que los posee, almacena o utiliza, cuando ello resulte procedente.
- Oposición: es el derecho que tiene el titular de solicitar que sus datos personales no se utilicen para ciertos fines, o de requerir que

[8] **Ejercicio de Derechos ARCO**: De conformidad con lo establecido en la fracción XI, de la Ley General.

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 (derechos ARCO), será substanciado por la Unidad de Transparencia, en términos de lo establecido en la Ley General, los Lineamientos Generales y el Acuerdo General.

Es indispensable que las instancias consulten el **Procedimiento de ejercicio de los derechos ARCO**, que constituye el **anexo III** de este documento.

Portabilidad de los datos personales

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

a) Aspectos Generales

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

A través del ejercicio de la portabilidad, los 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 y los Lineamientos para la Portabilidad.

b) Ejercicio del derecho de Portabilidad

En términos de lo previsto en el artículo 57 de la Ley General, 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. El titular hubiere proporcionado directamente al CJF sus datos personales de forma activa y consciente.

De modo que, de actualizarse los supuestos citados, el 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 para la Portabilidad, 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.

III. El formato sea interoperable con otros sistemas informáticos, esto es, que el CJF y la instancia receptora 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 citados, la portabilidad de los datos personales ante el CJF, tendrá por objeto que el titular pueda solicitar:

- Una copia de los datos personales que hubiere facilitado directamente a una instancia, en un formato estructurado y comúnmente utilizado, que le permita seguir utilizándolos y, en su caso, entregarlos a una instancia diversa del CJF para su reutilización y aprovechamiento en un nuevo tratamiento.
- La transmisión de sus datos personales a una instancia receptora diversa del CJF, siempre y cuando sea técnicamente posible, el titular hubiere facilitado directamente sus datos personales a la instancia transmisora 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 el artículo 14 de los Lineamientos para la Portabilidad, **en relación** con los numerales 51, 52, octavo párrafo de la Ley General, y 27, fracción I, de dichos lineamientos, la atención de las solicitudes de portabilidad de los datos personales **se realizará a través de la Unidad de Transparencia del CJF**.

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 para la Portabilidad, así como los criterios y parámetros establecidos en la Ley General, Lineamientos Generales y Acuerdo General para el ejercicio de los derechos ARCO.

Por lo anterior, en caso de que alguna de las instancias del CJF 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**.

Ciclo de vida de los datos personales

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

De conformidad con la fracción I del artículo 33 de la Ley General, 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, estipula 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 vida de los datos personales

De ese modo, en los términos declarados en el Inventario de Datos Personales y Sistemas[9], **en cada tratamiento** las instancias deberán realizar lo siguiente:

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

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

[9] El Inventario de Datos Personales y Sistemas forma parte del Documento de Seguridad.

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

c) **Etapa de Archivo:** las relativas al archivo del documento, en los términos previstos, respectivamente, en:

   i. El Acuerdo de Archivo Jurisdiccional.

   ii. El Acuerdo de Archivo Administrativo.

d) **Etapa de eliminación**: las acciones relativas a la baja documental o, en su caso, su destrucción, en los términos señalados en los referidos acuerdos generales[10].

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, 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.

[10] Véase el capítulo correspondiente a la *Supresión de los datos personales* en este documento.

Una vez transcurrido el bloqueo de los datos personales, procederá su eliminación, de conformidad con el procedimiento de baja archivística que la Dirección General de Archivo y Documentación prevea para dicho propósito.

Al respecto, el bloqueo de los datos personales corresponderá a los periodos máximos de vigencia documental[11], o en su caso, a los plazos de conservación[12], previstos en los artículos 25 y 26 del Acuerdo de Archivo Administrativo.

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 y el presente Programa de Protección de Datos Personales.

---

11 **Vigencia documental:** Periodo durante el cual un documento de archivo mantiene sus valores administrativos, legales, fiscales o contables, de conformidad con las disposiciones jurídicas vigentes y aplicables.

12 **Plazo de conservación:** Al periodo de guarda de la documentación en los archivos de trámite y concentración, que consiste en la combinación de la vigencia documental y, en su caso, el término precautorio y periodo de reserva que se establezcan de conformidad con la normatividad aplicable.

Supresión de datos personales

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

En términos de lo establecido en el artículo 23 de la Ley General, 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 los Lineamientos Generales estipula 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 la Ley General y los Lineamientos Generales.
- **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, las instancias deberán suprimir los datos personales de conformidad con lo que se expone a continuación.

a) Supresión de los datos personales en áreas administrativas

De conformidad con lo establecido en el Acuerdo de Archivo Administrativo, las áreas administrativas deberán realizar lo siguiente:

1. Mantener identificados los plazos de conservación de las series documentales que contienen datos personales.
2. En términos de lo dispuesto en el artículo 38 del Acuerdo de Archivo Administrativo, realizar la destrucción de los documentos correspondientes a dichas series 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 en términos de lo establecido en el artículo 42 del Acuerdo de Archivo Administrativo, a los documentos electrónicos, que son aquellos en los que las áreas administrativas 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.

b) Supresión de los datos personales en órganos jurisdiccionales.

De conformidad con el Acuerdo General del Pleno del Consejo de la Judicatura Federal, que establece las disposiciones en materia de valoración, depuración, destrucción, digitalización, transferencia y resguardo de los expedientes judiciales generados por los órganos jurisdiccionales (Acuerdo de Archivo Jurisdiccional), los órganos jurisdiccionales deberán realizar los siguiente:

1. Mantener identificados los plazos de conservación de las series documentales que contienen datos personales.
2. En términos de lo dispuesto en los artículos 18 y 24 del Acuerdo de Archivo Jurisdiccional, realizar la depuración o destrucción[13] 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.

[13] **Depuración:** procedimiento consistente en retirar aquellos documentos que no son parte del procedimiento, trámite o gestión que integra el expediente, o bien que carecen de valores documentales.

Destrucción: procedimiento mediante el cual se realiza la desincorporación y desintegración material total de los expedientes judiciales y auxiliares.

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 INAI.

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 INAI, 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 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 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 continúo 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, recibiéndolos 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 asegurar la debida protección de los datos personales, conforme al sistema jurídico mexicano en la materia.
- 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 instancias 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 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 INAI 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 INAI.

d) Informe de exención

Cuando a juicio de la Unidad de Transparencia 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.

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 de los Lineamientos para le Evaluación de Impacto, lo que se hará del conocimiento del Comité de Transparencia.

Capacitación

Este apartado se refiere a la capacitación que deberá otorgarse a los servidores públicos del CJF en materia de protección de datos personales.

El Comité de Transparencia y la Unidad de Transparencia, con apoyo del Instituto de la Judicatura Federal, deberán establecer un programa anual de capacitación y actualización en materia de protección de datos personales, el cual, de conformidad con los artículos 92 de la Ley General, así como 48 y 64 de los Lineamientos Generales, deberá dirigirse a todas las instancias del Consejo de la Judicatura Federal, diseñado a corto, mediano y largo plazo, considerando los roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de los puestos respectivos.

En ese sentido, a propuesta de la Unidad de Transparencia, en coordinación con el Instituto de la Judicatura Federal, el Comité deberá aprobar anualmente el programa de capacitación de datos personales.

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 y 63 de los Lineamientos Generales, las políticas y directrices planteadas en este programa deberán ser supervisadas, monitoreadas y revisadas a través de auditorías y revisiones administrativas, cuestión que será efectuada por la Unidad de Transparencia al implementar los *Mecanismos de Monitoreo, Revisión, Alertas, Vulneraciones y Auditoría*, que obran en el Documento de Seguridad (**anexo I**).

Procedimiento de orientación y quejas

Este apartado se refiere a los mecanismos disponibles para orientar a los 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, 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, estipula 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, los 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 en modalidad virtual y física.

a) Modalidad Virtual.

Se implementará mediante un buzón electrónico, por el que los titulares de los datos personales podrán exponer a detalle sus dudas,

cuestionamientos y quejas, mismas que serán atendidas por la Secretaría de Protección de Datos Personales.

Con apoyo de la Dirección General de Tecnologías de la Información, el buzón deberá encontrarse habilitado permanentemente en el micrositio de la Unidad de Transparencia en el Portal de Internet del Consejo.

b) Modalidad física

La oficialía de partes de la Unidad de Transparencia, informará a los 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 les aquejen respecto del tratamiento respectivo.

La atención de tales cuestionamientos, corresponderá a la Secretaría de Protección de Datos Personales, 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 que emite la Secretaría de Protección de Datos Personales, los cuales 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.

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 CJF.

Con la finalidad de que el presente Programa 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 las instancias, 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 este Programa.

Por tanto, una vez ejecutados los *Mecanismos de Monitoreo, Revisión, Alertas, Vulneraciones y Auditoría*[14], los puntos de mejora advertidos deberán ser sometidos a conocimiento del Comité de Transparencia.

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

[14] Localizado en el Documento de Seguridad.

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.

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

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.

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**.

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.