GUÍA BÁSICA PARA EL CUMPLIMIENTO DE PRINCIPIOS Y DEBERES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN EL SECTOR EDUCATIVO

Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Guerrero

09 DE JULIO DE 2020

P R E S E N T A C I Ó N

El derecho humano de protección de datos personales es reconocido por la Constitución Política de los Estados Unidos Mexicanos en el segundo párrafo del artículo 16 constitucional, estableciendo que *toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.*

Es decir que, al establecer el derecho de protección de datos personales como una garantía constitucional se establece el respeto irrestricto, salvo excepciones de la legislación aplicable, dotando a cualquier persona física sin distinción de origen étnico, religión, preferencia sexual o cualquier otra característica, el control sobre el uso de sus datos personales a través del ejercicio de los derechos ARCO.

La legislación específica regulatoria en el sector público actualmente comprende la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley número 466 de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Guerrero para el caso de la Entidad, mismas que establecen entre otras regulaciones, un conjunto de principios y deberes para los responsables que tratan los datos personales, principios: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad; y deberes: seguridad y confidencialidad; derechos ARCO para los titulares, acceder a sus datos, solicitar su rectificación en caso de que sean inadecuados o excesivos, pedir su cancelación, y manifestar su oposición al tratamiento, sumándose recientemente en este control sobre los datos personales, el derecho a la portabilidad.

No obstante, existe un desconocimiento generalizado en la población y si bien, no es necesariamente privativo del Estado de Guerrero, el Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Guerreo como órgano garante local del derecho humano de protección de datos personales cuenta con la facultad de elaborar material que coadyuve al cumplimiento de la legislación existente en la materia.

En este sentido, es menester brindar a responsables de datos personales herramientas que faciliten el cumplimiento de la legislación aplicable; El presente documento contempla las actividades básicas para el cumplimiento de principios y deberes en materia de protección de datos personales, señaladas en México por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y específicamente en Guerreo por la Ley número 466 de Protección de Datos Personales en Posesión de Sujetos Obligados en el Estado de Guerrero.

Adicional a lo anterior, las y los titulares de los datos personales deben conocer y cuidar la información relativa a sus datos personales para un libre ejercicio del mismo, que les permita tener un control del uso de su información personal desde el momento de su emisión, el derecho de protección de datos personales inicia desde el uso adecuado por parte del titular; hablamos de una responsabilidad compartida para un bienestar común.

CONCEPTOS BÁSICOS

I. **Aviso de privacidad:** Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos;
II. **Bases de datos:** Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;
III. **Bloqueo:** La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;
IV. **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;
V. **Consentimiento:** Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos;
VI. **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;
VII. **Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;
VIII. **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

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

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

XI. **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;

XII. **LGPDPPSO:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

XIV. **Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

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

XVI. **Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

XVII. **Oficial:** La persona encargada de las funciones relativas a la protección de los datos personales dentro del responsable, establecidas en la norma aplicable;

XVIII. **Responsable:** Son sujetos obligados en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos que deciden sobre el tratamiento de datos personales;

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

XX. **Titular:** La persona física a quien corresponden los datos personales;

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

XXII. **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, y

2. PRINCIPALES FIGURAS

2.1 Responsable de datos personales

Son sujetos obligados en el ámbito estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos que deciden sobre el tratamiento de datos personales.

Los centros educativos de orden público serán los responsables del tratamiento de datos personales a través de la Secretaría de Educación Guerrero y demás responsables en el sector educativo competentes en la materia.

2.2 Oficial de Protección de Datos Personales

Aquellos responsables que en el ejercicio de sus funciones sustantivas lleven a cabo tratamientos de datos personales **relevantes o intensivos**, podrán designar a un oficial de protección de datos personales.

El oficial de protección de datos personales tendrá las siguientes atribuciones:

- Asesorar al Comité de Transparencia respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales;
- Diseñar, ejecutar, supervisar y evaluar políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley de la materia y demás disposiciones que resulten aplicables en la materia, en coordinación con el Comité de Transparencia;
- Asesorar permanentemente a las áreas adscritas al responsable en materia de protección de datos personales;
- Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;
- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
- Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
- Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;
- Guardar confidencialidad respecto de los datos personales tratados;

2.3 Encargado

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.

El encargado deberá realizar las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitar sus actuaciones a los términos fijados por el responsable.

La relación entre el responsable y el encargado deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa que le resulte aplicable, y que permita acreditar su existencia, alcance y contenido.

En el contrato o instrumento jurídico que decida el responsable se deberán prever, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste el encargado:

I. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;
II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
IV. Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;
V. Guardar confidencialidad respecto de los datos personales tratados;
VI. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y
VII. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente. Los acuerdos entre el responsable y el encargado relacionados con el tratamiento de datos personales no deberán contravenir la Ley de la materia y demás disposiciones aplicables, así como lo establecido en el aviso de privacidad correspondiente.

3. PRINCIPIOS Y DEBERES

3.1 Principios

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

Los centros educativos recolectan datos personales de estudiantes, padres de familia o demás figuras jurídicas a cargo del bienestar de menores, es menester insistir en las acciones que garanticen el respeto al derecho humano de protección de datos personales.

Los centros educativos también podrán llevar a cabo el tratamiento de datos personales cuando:

- sea necesario para el cumplimiento de la relación jurídica que se establezca con la matrícula.
- se disponga del consentimiento de los titulares o representante legal acreditado.
- pueda existir un interés legítimo que prevalezca sobre los derechos y libertades de los titulares.

3.1.1 Licitud

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

El principio de licitud refiere a la obligación del responsable de recabar y dar tratamiento a los datos personales de forma lícita conforme a las disposiciones establecidas en la normatividad de datos personales aplicable.

Este principio implica el mandato de que el responsable del tratamiento de los datos personales lleve a cabo el tratamiento con apego y cumplimiento a lo dispuesto por la legislación aplicable, el responsable deberá abstenerse de realizar tratamientos para los que no esté facultado.

3.1.2 Finalidad

El principio de finalidad se traduce en la obligación legal a cargo del responsable de tratar los datos personales del titular exclusivamente para dar cumplimiento a las finalidades que le fueron informadas al titular mediante el aviso de privacidad del responsable.

Todo tratamiento de datos personales que efectúe el responsable deberá estar facultado por la normativa aplicable y justificado por finalidades:

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 con el titular.

Explícitas: se deberán especificar de manera clara para qué objeto se tratarán los datos personales, sin lugar a confusión y con objetividad. El responsable se encuentra obligado a evitar que las finalidades que describa en el aviso de privacidad sean inexactas, ambiguas o vagas e incluyan redacciones como “de manera enunciativa más no limitativa”, “entre otras finalidades”, “otros fines análogos”, “por ejemplo” o “entre otros”.

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 que le resulte aplicable.

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 la LGPDPPSO.

Por otro lado, la finalidad o finalidades del tratamiento se distinguen en dos tipos:

- **primarias:** las que dan origen a la relación jurídica entre el responsable y el titular y

- **secundarias:** las que no dan origen a la relación jurídica y están sometidas al consentimiento del titular, sin que la negativa de éste tenga como consecuencia la conclusión del tratamiento.

  En el aviso de privacidad se deberá informar al titular sobre el mecanismo implementado para que pueda manifestar su negativa para el tratamiento de sus datos personales en relación con las finalidades que no son necesarias para la relación jurídica entre el responsable y titular.

3.1.3 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.

3.1.4 Consentimiento

El responsable deberá contar con el **consentimiento previo** del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

I. Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular;

II. Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento, e

III. Informada: Que el titular tenga conocimiento del **aviso de privacidad previo al tratamiento** a que serán sometidos sus datos personales.

Menores de edad o personas en estado de interdicción o incapacidad.

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la normativa aplicable, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.

El consentimiento podrá manifestarse de forma expresa o tácita.

Se deberá entender que el consentimiento es **expreso** cuando la voluntad del titular se manifieste verbalmente, **por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.**

El consentimiento será **tácito** cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste **no manifieste su voluntad en sentido contrario**. Por regla general será válido el consentimiento tácito, salvo que la norma o disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente.

Tratándose de **datos personales sensibles** el responsable deberá obtener el **consentimiento expreso y por escrito del titular** para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 22 de la LGPDPPSO.

Consentimiento Expreso

De acuerdo con la normatividad de datos personales, dichas características del consentimiento expreso consisten en lo siguiente:

- **Libre:** cuando el consentimiento expreso es obtenido sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular.
- **Específico:** cuando el consentimiento expreso se refiere de forma concreta, explícita y lícita a una o varias finalidades determinadas que justifiquen el tratamiento de los datos personales. Este requisito se cumple cuando la solicitud del consentimiento va relacionada con las finalidades concretas del tratamiento que se informan en el aviso de privacidad. Es decir, en base de esta característica, el consentimiento se debe solicitar para tratar los datos personales para finalidades específicas, no en lo general.
- **Informado:** cuando de forma previa al otorgamiento del consentimiento, se hace del conocimiento del titular de los datos personales, el aviso de privacidad en virtud del cual se informa sobre el tratamiento al que serán sometidos los datos personales y las consecuencias de otorgar su consentimiento.

Se considera que el consentimiento expreso se ha otorgado por escrito en el momento en el que el titular externa su voluntad mediante un documento que contiene su firma autógrafa, huella dactilar, firma electrónica, firma electrónica avanzada.

Además de lo anterior, el consentimiento es revocable, de modo que el titular tiene la posibilidad de revocarlo en cualquier momento y el responsable, la correlativa obligación de establecer mecanismos sencillos y gratuitos que le permitan al titular

ejercer dicho derecho (al menos por el mismo medio por el que lo otorgó) siempre y cuando no lo impida una disposición legal.

En cuanto a los supuestos en los que es obligatorio obtener un consentimiento expreso, y no así uno tácito, podemos señalar los siguientes:

- *Lo exija una ley o reglamento*
- *Se trate de datos financieros o patrimoniales*
- *Se trate de datos sensibles*
- *Lo solicite el responsable para acreditar el mismo*
- *Lo acuerden así el titular y el responsable*

Consentimiento Tácito

Las características del consentimiento tácito consisten en lo siguiente:

- **Libre:** cuando el consentimiento expreso es obtenido sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular.
- **Específico:** cuando el consentimiento se refiere de forma concreta, explícita y lícita a una o varias finalidades determinadas que justifiquen el tratamiento de los datos personales. Es decir, como lo indican las autoridades de la materia, la solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informen en el aviso de privacidad, es decir, el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas, no en lo general.
- **Informado:** cuando de forma previa al otorgamiento del consentimiento, se hace del conocimiento del titular de los datos personales el aviso de privacidad en virtud del cual se informa sobre el tratamiento al que serán sometidos los datos personales y las consecuencias de otorgar su consentimiento.
- **Inequívoco:** de acuerdo con la normatividad, este requisito se cumple cuando existen elementos que de manera indubitable demuestran que el mismo ha sido lícitamente otorgado por el titular.

En ausencia de dichas características, el consentimiento no puede considerarse como lícitamente otorgado.

Además de lo anterior, el consentimiento es revocable, de modo que el titular tiene la posibilidad de revocarlo en cualquier momento, y el responsable, la correlativa obligación de establecer mecanismos sencillos y gratuitos que permitan al titular ejercer dicho derecho al menos por el mismo medio por el que lo otorgó, siempre y cuando no lo impida una disposición legal.

El consentimiento tácito generalmente es válido para cualquier tipo de dato personal con excepción de aquellos datos que revistan el carácter de datos personales

patrimoniales, financieros o sensibles pues en dicho caso se deberá contactar personal o directamente al titular para requerir el consentimiento respectivo; no obstante el consentimiento tácito también es susceptible de estar excepcionado bajo los supuestos previstos en los artículos 22 y 70 de la LGPDPPSO.

3.1.5 Calidad

El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

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

El principio de calidad está estrechamente relacionado con el principio de finalidad, y proporcionalidad, puesto que se materializa cuando los datos personales tratados son exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la que se tratan. En relación con la concreción práctica de estos elementos, el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales precisa que los mismos tienen el siguiente alcance:

Exactos: se considera que los datos personales son exactos cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles.

Completos: se considera que los datos personales están completos cuando no falta ninguno de los que se requieran para las finalidades para las cuales se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio al titular.

Pertinentes: se considera que los datos personales son pertinentes cuando corresponden efectivamente al titular.

Actualizados: se considera que los datos personales están actualizados cuando están al día y corresponden a la situación real del titular.

Correctos: se considera que los datos personales son correctos cuando cumplen con todas las características anteriores.

El principio de calidad entraña distintas obligaciones:

- conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos, y el periodo de bloqueo;
- cancelar los datos personales una vez cumplida la finalidad del tratamiento, entendiendo que la cancelación da lugar al bloqueo, y a éste luego le seguirá la supresión.

- fijar y documentar los plazos de conservación y
- acreditar que dichos plazos de conservación sean cumplidos por el responsable.

Conservación

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los **aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales**.

Establecimiento de los plazos de conservación, deberán considerar con lo siguiente:

- no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron el tratamiento;
- deberán atender las disposiciones aplicables a la materia de que se trate;
- deberán tomar en cuenta los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información y
- el período de bloqueo de éstos.

En consecuencia, para determinar el plazo de conservación de los datos personales, el responsable deberá tomar en cuenta lo siguiente:

- plazo de conservación;
- tiempo requerido para levar a cabo las finalidades del tratamiento;
- plazos legales, administrativos, contables, fiscales, jurídicos e históricos aplicables y
- periodo de bloqueo

3.1.6 Proporcionalidad

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

El principio de proporcionalidad impone al responsable del tratamiento un límite en la recolección de datos personales, de forma tal que el responsable no recabe datos personales a su arbitrio y, sin que sean necesarios para el cumplimiento de un fin concreto, explícito y legítimo.

Por ejemplo, si se requiere la identificación para finalidades de acreditación de identidad pero no es necesario conocer datos de localización, se puede solicitar otra identificación oficial como la cedula profesional.

3.1.7 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**.

Tipos de aviso de privacidad:

1. Aviso simplificado

2. Aviso integral

Momento de informar

La obligación de informar a las personas interesadas sobre las circunstancias relativas al tratamiento de sus datos recae sobre el Responsable del Tratamiento.

El responsable deberá poner a disposición del titular **el Aviso de Privacidad simplificado** en los siguientes momentos:

I. Cuando los datos personales se obtienen de manera directa del titular previo a la obtención de los mismos, y

II. Cuando los datos personales se obtienen de manera indirecta del titular previo al uso o aprovechamiento de éstos.

Las reglas anteriores, no eximen al responsable de proporcionar al titular el Aviso de Privacidad integral en un momento posterior, conforme a las disposiciones aplicables de la LGPDPPSO.

Medios para informar

La recolección de los datos personales ocurre cuando el titular proporciona personalmente sus datos personales a quien representa al responsable o a través de algún medio que permita su entrega directa como podrían ser sistemas o medios electrónicos, ópticos, sonoros, visuales, vía telefónica, internet o cualquier otra tecnología o medio físico, es decir los procedimientos de recolección de información pueden ser distintos y, en consecuencia, los modos de informar a los titulares deben adaptarse a las circunstancias de cada uno de los medios empleados para la recolección o registro de los datos.

Siendo las situaciones antes citadas algunas de las formas más habituales de recolección de datos y, en consecuencia, a través de los cuales hay que informar, pueden ser:

- Formularios en papel
- Vía telefónica
- Navegación o formularios web
- Registro de aplicaciones móviles
- Grabaciones

Por otra parte, los mecanismos de difusión o reproducción del aviso de privacidad al titular sobre datos ya disponibles, o tratamientos adicionales, pueden hacerse llegar, entre otros, por medio de:

- Formatos físicos

- Formatos electrónicos
- Medios verbales

O cualquier otra tecnología, siempre y cuando garantice y cumpla con la información a que se refiere la LGPDPPSO.

Las características de cada uno de los medios varían en cuanto a extensión, disponibilidad de espacio, legibilidad, posibilidad de vincular informaciones, etc. En cualquier caso**,** el Aviso de Privacidad deberá caracterizarse por**:**

Ser sencillo, con información necesaria, expresado en lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.

En el Aviso de Privacidad queda **prohibido**:

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

Aviso de Privacidad Simplificado

Dar a conocer la información básica sobre el tratamiento que recibirán los datos personales de los titulares debe estar vertida en el aviso de privacidad simplificado, en el mismo momento y en el mismo medio en que se recolecten los datos con un contenido mínimo la siguiente información:

Tema	Especificaciones
Denominación del responsable	Nombre completo del responsable de los datos personales
Finalidades	Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular. *Datos personales sensibles
Transferencias de datos personales que requieran consentimiento	Se deberá informar: 1. Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales de carácter privado a las que se transfieren los datos personales, y 2. Las finalidades de estas **transferencias**;
Mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su **negativa**	Los mecanismos y medios deberán estar disponibles al titular previo a que ocurra dicho tratamiento.

para el tratamiento de sus datos personales **para finalidades y transferencias** de datos personales que requieren el consentimiento del titular	
Sitio donde se podrá consultar el Aviso de Privacidad Integral.	La puesta a disposición del Aviso de Privacidad Simplificado no exime al responsable de su obligación de proveer los mecanismos para que el titular pueda conocer el contenido del aviso de privacidad integral en un momento posterior.

Aviso de privacidad integral

El contenido del aviso de privacidad integral se manifiesta de manera detallada y clara con la finalidad de que los titulares conozcan a detalle el tratamiento de sus datos personales una vez en posesión del responsable.

Tema	Especificaciones
Denominación del responsable	Nombre completo del responsable de los datos personales
Domicilio del responsable	Ubicación completa del domicilio del responsable
Finalidades	Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular. *Datos personales sensibles
Los datos personales que serán sometidos a tratamiento	Se deberá identificar aquéllos que sean sensibles;
El fundamento legal que faculta expresamente al responsable para llevar a cabo:	1. El tratamiento de datos personales, y
	2. Las transferencias de datos personales que, en su caso, efectúe con autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales de carácter privado.
Transferencias de datos personales que requieran consentimiento	Se deberá informar: 1. Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales de carácter privado a las que se transfieren los datos personales, y 2. Las finalidades de estas **transferencias**;

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 el consentimiento del titular	Los mecanismos y medios deberán estar disponibles al titular previo a que ocurra dicho tratamiento.
Los mecanismos, medios y procedimientos disponibles para ejercer los derechos **ARCO**	Cómo ejercer los derechos de acceso, rectificación, cancelación u oposición o bien portabilidad de sus datos.
El domicilio de la Unidad de Transparencia	Datos de localización para el ejercicio de derechos ARCO o bien portabilidad.
Cambios en el aviso de privacidad	Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.
Fecha	Fecha de elaboración o de última actualización del aviso de privacidad

Recomendaciones para el aviso de privacidad

La forma de presentación preferente de este primer aviso es de manera resumida, garantizando que dicha información quede “a la vista” del interesado, según sea el medio utilizado en la recolección de la información.

- **Debe estar claramente identificada bajo un título como “Aviso de Privacidad”**

Por ejemplo, en un formulario de solicitud, el texto con la información básica debería situarse en el mismo campo de visión que el lugar donde haya de manifestarse la conformidad con lo solicitado (la firma, si es en papel, o el botón de “enviar”, si es un formulario electrónico).

- **Finalidades**

Las finalidades de todo tratamiento de datos personales deben tener finalidades concretas, explícitas lícitas y legítimas que justifiquen su tratamiento, mismas que deben ser descritas ampliamente en el aviso de privacidad. Distinguiendo aquéllas que requieran el consentimiento del titular.

- **Datos personales que serán sometidos a tratamiento**

El listado de los datos personales objeto del tratamiento, ya sean separados por categorías o en un mismo listado, debiendo identificar aquéllos que sean sensibles.

- **Fundamento legal que faculta expresamente al responsable para llevar a cabo el tratamiento de los datos personales y su transferencia en su caso.**

El fundamento legal que faculta al responsable para llevar a cabo el tratamiento, con independencia de que se requiera o no el consentimiento (incluir artículos, apartados, fracciones, incisos y nombre de los ordenamientos o disposición normativa vigente que lo faculta o le confiera atribuciones para realizar el tratamiento de datos personales que informa en el aviso de privacidad, precisando su fecha de publicación o, en su caso, la fecha de la última modificación).

- **Transferencias de datos personales que requieran consentimiento**

Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:

1. **Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales de carácter privado a las que se transfieren los datos personales, y**

2. **Las finalidades de estas transferencias;**

Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en LGPDPPSO y deberá ser informada al titular en el Aviso de Privacidad, así como limitarse a las finalidades que las justifiquen.

Se recomienda observar lo dispuesto en el Título Sexto Comunicaciones de datos personales, Capítulo Único Transferencias de datos personales de la LGPDPPSO.

- **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 el consentimiento del titular**

Por ejemplo, en un formulario de solicitud, el texto con la información básica debería situarse en el mismo campo de visión que el lugar donde haya de manifestarse la conformidad con lo solicitado (la firma, si es en papel, o el botón de "enviar", si es un formulario electrónico).

- **Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO**

En todo momento el titular o su representante podrán solicitar al responsable el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen, de conformidad con la LGPDPPSO.

El ejercicio de cualquiera de los derechos ARCO no es requisito previo, ni impide el ejercicio de otro.

I. Derecho de acceso.

El titular tendrá derecho de acceder a sus datos personales que obren en posesión del responsable, así como a conocer la información relacionada con las condiciones, generalidades y particularidades de su tratamiento.

II. Derecho de rectificación.

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.

III. Derecho de cancelación.

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.

Aplican excepciones, se recomienda observar lo establecido en la LGPDPPSO.

IV. Derecho de oposición.

El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, de conformidad a lo dispuesto en la LGPDPPSO.

Aplican excepciones, se recomienda observar lo establecido en la LGPDPPSO.

V. 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 personales objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado, el cual le permita seguir utilizándolos.

Se recomienda observar lo establecido en LGPDPPSO y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

- **El domicilio de la Unidad de Transparencia**

Se recomienda plasmar la información de localización precisa de la unidad de transparencia, señalando calle, número, colonia o fraccionamiento, ciudad, municipio, código postal y entidad federativa, así como su número y extensión

telefónica, página web oficial de consulta y demás información que facilite la localización del responsable.

En caso de contar con oficial de protección de datos personales, se recomienda adjuntar los datos de localización y comunicación, especialmente para el caso de la recolección de datos personales sensibles.

- **Cambios en el aviso de privacidad**

Ejemplo: Cuando el responsable pretenda tratar los datos personales para una finalidad distinta, deberá poner a su disposición un nuevo Aviso de Privacidad con las características del nuevo tratamiento previo al aprovechamiento de los datos personales para la finalidad respectiva.

Ejemplos de la comunicación del aviso de privacidad

En papel:

- *En el mismo formulario (por ejemplo, en la parte baja del archivo, complementando al reverso de ser necesario)*
- *Como un anexo o que se entregue al interesado y que pueda conservar*
- *Como información expuesta, claramente visible, en carteles, paneles, trípticos, etc, de los cuales se pueda solicitar una copia manejable para conservar.*

Medios electrónicos:

- *En una página web específica, a la que se accede mediante un hipervínculo*
- *Como un documento disponible para su descarga desde una URL*
- *Como información anexa o adjunta a un mensaje electrónico dirigido al interesado*

Comunicación telefónica:

- *Como un mensaje que se le ofrezca al titular, como complemento o alternativa a una oferta de disponibilidad del aviso integral accesible electrónicamente o remitida, por correo postal o electrónico.*

Obtención de datos personales por parte de un tercero

La procedencia de los datos en el supuesto de que los datos personales no se hayan obtenidos del titular, por proceder de alguna excepcionalidad establecida por la normativa aplicable, o derive de fuentes de acceso público.

Los medios para facilitar esta información serán, normalmente, diferentes a los utilizados para informar en el momento de recolectar los datos. Los más adecuados pueden ser:

- Correo postal

- Correo electrónico
- cualquier medio que manifieste que el consentimiento expreso se otorgó, ya sea por escrito cuando el titular lo externe mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por la normativa aplicable. En el entorno digital, podrán utilizarse medios como la firma electrónica o cualquier mecanismo o procedimiento equivalente que permita identificar fehacientemente al titular, y a su vez, recabar su consentimiento de tal manera que se acredite la obtención del mismo.

Habrá de ponderarse la adecuación del medio con la necesidad de poder demostrar que se ha dado cumplimento al deber de informa.

En el caso del correo postal o del correo electrónico, la práctica que se sugiere como más adecuada es:

- *Incorporar el aviso de privacidad simplificado en la propia notificación donde se le informa al interesado del tratamiento.*
- *Adjuntar el aviso de privacidad integral como un anexo*
- *Opcionalmente, incluir una vinculación a la información adicional en forma electrónica*

Lo anterior, en un formato diseñado para que el titular manifieste su consentimiento expreso, si así lo desea.

El responsable deberá considerar la procedencia de notificar la información adicional, en este caso:

- La fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público disponibles sin restricciones.
- Las categorías de datos personales de que se trate, con especial indicación de los datos especialmente protegidos, como lo son los datos sensibles.

No solo será importante contar con el aviso de privacidad, sino darle una debida difusión. Algunas de las obligaciones que impone la normatividad en relación con la debida difusión del aviso de privacidad se encuentran las siguientes: difundirlo por medios electrónicos y físicos y ubicarlo en un lugar visible que facilite la consulta del titular y que le permita acreditar fehacientemente el cumplimiento de esta obligación ante la autoridad competente.

Es importante considerar que al presentarse una controversia entre el titular y el responsable de la información respecto de la acreditación de la puesta a disposición del aviso de privacidad, quien tendrá la carga probatoria será, el responsable.

Medidas compensatorias

Cuando resulte imposible dar a conocer al titular el aviso de privacidad de manera directa o ello exija esfuerzos desproporcionados, el responsable podrá instrumentar medidas compensatorias de comunicación masiva, *se recomienda observar lo*

establecido en la LGPDPPSO, así como los Criterios Generales para la Instrumentación de Medidas Compensatorias en el Sector Público del orden federal, estatal y municipal.

3.1.8 Responsabilidad

El principio de responsabilidad es aquel que obliga al responsable a implementar específicos mecanismos legales para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la LGPDPPSO y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular, a la autoridad competente. El responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la normatividad aplicable, así como establecer aquellos mecanismos necesarios para evidenciar dicho cumplimiento ante los titulares y la autoridad competente.

Cumplimiento

Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad están al menos, los siguientes:

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

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

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

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

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

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

VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la LGPDPPSO y las demás que resulten aplicables en la materia, y

VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que

implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la LGPDPPSO y las demás que resulten aplicables en la materia.

3.2 DEBERES

Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

3.2.1 Confidencialidad

El deber de confidencialidad es la obligación que tiene una entidad de resguardar la confidencialidad de lo que tiene bajo responsabilidad o custodia.

El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de estos, obligación que subsistirá aún después de finalizar sus relaciones con el titular o, en su caso, con el responsable.

Los responsables y encargados del tratamiento de los datos personales a lo largo del ciclo de vida e independientemente de su ubicación y de los sistemas empleados para su tratamiento, deben implementar mecanismos de seguridad de carácter administrativo, físico o técnico.

Los mecanismos de seguridad del tipo administrativo implican realizar cambios en la asignación de roles y responsabilidades de las personas que tratan datos personales, utilización de instrumentos jurídicos, programas de capacitación y concientización, entre otros.

Como los datos personales pueden estar contenidos en cualquier medio y en diferentes formatos, no solamente en forma electrónica en sistemas informáticos, los mecanismos de seguridad físico para garantizar el deber de confidencialidad incluyen medidas de control de acceso físico a los datos personales.

Por otro lado, los mecanismos de seguridad de carácter técnico implican el uso de infraestructura tecnológica para garantizar el deber de confidencialidad en los datos personales en cualquier etapa del ciclo de vida de su tratamiento. En forma general, los mecanismos de seguridad técnicos para garantizar la confidencialidad se clasifican en:

a) Mecanismos de cifrado

b) Mecanismos de control de acceso

c) Mecanismos de prevención de fuga de datos

3.2.2 Seguridad

De acuerdo a lo establecido en la LGPDPPSO, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

En este sentido el deber de seguridad se cumple con la implementación y mantenimiento de medidas de seguridad en todas las fases del ciclo de vida en donde se traten los datos personales y exista algún riesgo de vulneración hacia los mismos.

Acciones principales

La implementación de las medidas de seguridad se realiza a través de un proceso de gestión sistemático que abarca como mínimo las siguientes tareas:

I. Crear políticas de seguridad internas.

Las políticas de seguridad se crean bajo el marco normativo de la organización, alineadas a los requerimientos legales de carácter nacional o internacional.

II. Identificar el tipo de datos personales tratados en la organización.

La identificación del tipo de datos personales manejados a lo largo del flujo de información en los procesos de la organización es importante porque, **dependiendo de la sensibilidad de los datos, será el tipo de medida de seguridad implementado**.

III. Identificar las personas y sistemas que hacen tratamiento de los datos personales.

La identificación de las personas y sistemas que hacen tratamiento de los datos personales permite validar si los roles y permisos asignados a las personas son los adecuados para el correcto tratamiento de los datos personales.

La identificación de los sistemas que tratan los datos, permite visualizar en que parte del ciclo de vida y la forma en que los datos son creados, almacenados, usados y eliminados.

IV. Realizar un análisis de riesgo.

El análisis de riesgo es un proceso que ayuda a identificar escenarios de riesgo de los datos personales, es decir, identificar todas las amenazas que pueden causar algún daño a los datos personales. Las amenazas son entidades o eventos que de

manera accidental o intencional afectan la confidencialidad, integridad o disponibilidad de los datos personales.

V. Efectuar un análisis de brecha.

El siguiente paso en el proceso de análisis de riesgo consiste en identificar las vulnerabilidades existentes alrededor del tratamiento de los datos personales. Las vulnerabilidades pueden ser de origen tecnológico, de procedimiento o de gente. El nivel de exposición de las vulnerabilidades depende de la existencia o falta de mecanismos de seguridad actualmente implementados.

VI. Identificar las medidas de seguridad y hacer un plan de implementación.

Una vez identificados los componentes del riesgo, se procede a evaluar el riesgo asignando un valor cualitativo o cuantitativo al escenario de riesgo. El resultado del proceso de análisis de riesgo es una lista evaluada y priorizada de escenarios de riesgo.

VII. Ejecutar programas de capacitación según el rol y nivel de responsabilidad del personal.

Se sugiere consultar lo establecido en la LGPDPPSO en su Capítulo II para mayor información respecto a las medidas de seguridad administrativas, físicas y técnicas.

4. TRATAMIENTO DE DATOS POR LOS CENTROS EDUCATIVOS

Los Centros Educativos tienen como propósito esencial crear condiciones que permitan asegurar el acceso, de las mexicanas y mexicanos, a una educación de excelencia con equidad, universalidad e integralidad, en el nivel y modalidad que la requieran y en el lugar donde la demanden, misión para la que han de tratar sus datos de carácter personal, así como los de sus padres y tutores. Este tratamiento se inicia desde el mismo momento en el que se solicita el ingreso a un centro. Trámite para el cual se realiza múltiples llenados de cuestionarios, así como la entrega de documentación con datos de carácter sensibles, mismos que se mantienen durante toda su estancia en el centro, e incluso una vez que haya finalizado sus estudios mediante la conservación del expediente académico.

4.1 Recolección de datos personales por los centros educativos

En el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior de la niña, el niño y el adolescente, en términos de las disposiciones legales aplicables.

Datos que pueden recabar los centros educativos

Los centros pueden recabar datos de carácter personal para la función docente y orientadora de los alumnos en referencia a:

- El origen y ambiente familiar y social.

- Las características o condiciones personales físicas y psicológicas.
- El desarrollo y resultados de su escolarización.
- Las circunstancias cuyo conocimiento sea necesario para educar y orientar a los alumnos.

Los centros educativos pueden recabar y tratar los datos de la población estudiantil y de sus padres o tutores, incluyendo también las categorías especiales de datos, como los de salud, cuando fuesen necesarios para el desempeño de la función docente y orientadora.

Pero también hay que tener en cuenta una serie de cautelas:

- Los datos personales no podrán usarse para fines diferentes al educativo (función docente y orientadora).
- El profesorado y resto del personal que acceda a los datos personales de los alumnos o de sus familias está sometido al deber de confidencialidad.

Es importante tener en cuenta que no podrán recabarse datos que sean excesivos para dicha finalidad.

Tipos de datos

Datos sobre la situación familiar de los padres de los alumnos

Los centros educativos podrían recabar la información sobre la situación familiar de los alumnos, observando siempre los principios y deberes en materia de protección de datos personales.

Datos de salud

En la medida en que sean necesarios para el ejercicio de la función educativa o bien cuando así se justifique por la legislación aplicable.

La recolección de datos de salud deberá estar justificada y bajo el cumplimiento de los principios y deberes en materia de protección de datos personales, lo anterior no exime a los responsables de la observancia de la normativa aplicable para el caso de los menores de edad.

Se pueden distinguir los siguientes momentos:

- En la matriculación del alumno: discapacidades, enfermedades crónicas, TDAH, intolerancias alimentarias o alergias.
- Durante el curso escolar: el tratamiento médico que reciba un alumno a través del servicio médico o de enfermería del centro o los informes de centros sanitarios a los que se le haya trasladado como consecuencia de accidentes o indisposiciones sufridas en el centro o los informes de los equipos de orientación psicopedagógica.

Excepcionalmente

- Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria.

Imágenes de los alumnos para el expediente académico

Entre los datos que pueden recabar los centros educativos para el ejercicio de la función docente y orientadora sin consentimiento de los alumnos se pueden incluir sus fotografías a los efectos de identificar a cada alumno en relación con su expediente.

Datos para finalidades distintas de la función propiamente educativa

Al margen de la función educativa, los centros pueden recabar datos para otras finalidades legítimas, como puede ser la gestión de la relación jurídica derivada de la matriculación de los alumnos, o dar a conocer la oferta académica, participar con los alumnos en concursos educativos u ofrecer servicios deportivos, de ocio o culturales. En estos casos, se podrán recabar bien como consecuencia de la relación jurídica establecida con la matrícula o si media el consentimiento previo de los alumnos o de sus padres o tutores.

Además, con carácter previo a la obtención del consentimiento, lo anterior no excusa del cumplimiento del principio de información con el aviso de privacidad en sus dos modalidades.

Procedimiento de recolección

Cuando se recaban datos personales, es necesario informar a los interesados.

Siempre se debe informar, aunque no sea necesario obtener su consentimiento. Los centros educativos y los responsables han de informar del tratamiento de los datos personales mediante el aviso de privacidad.

Casos en los que es necesario el consentimiento de los alumnos o de sus padres o tutores.

El consentimiento, cuando es la causa que legitima el tratamiento, se ha de obtener con carácter previo a su recolección. Se puede incluir en el mismo documento impreso o formulario en el que se recaban los datos.

El consentimiento ha de ser inequívoco y específico, correspondiendo al centro educativo o el responsable acreditar su existencia.

Para los datos que hagan referencia al origen racial, a la salud o cualquier dato considerado sensible por la normativa aplicable, el consentimiento ha de ser expreso.

El consentimiento se puede recabar en el mismo registro de recolección de los datos bastaría con que el consentimiento se preste al comienzo de cada curso, sin que

sea necesario recabarlo nuevamente en cada actividad de tratamiento siempre que responda a la misma finalidad, por ejemplo, para los eventos que organice el centro.

Recolección de datos personales de los alumnos por parte de los profesores directamente

Sin perjuicio de los datos personales recabados por los centros educativos o el responsable al matricularse los alumnos, y que son facilitados a los profesores para el ejercicio de la función docente, cuando éstos recaben otros datos de carácter personal, como grabaciones de imágenes o sonido con la finalidad de evaluar sus conocimientos u otros datos relacionados con la realización de dichos ejercicios, o los resultados de su evaluación, estarían legitimados para hacerlo, en el marco de las instrucciones, protocolos o régimen interno que el centro educativo o el responsable haya adoptado.

Solicitud de datos personales de padres de los alumnos

Los datos de los padres de los alumnos se recaban por los centros al estar legitimados por la normativa aplicable, a cuya información podrán tener acceso los profesores si la necesitarán para el ejercicio de la docencia.

No obstante, si se diera alguna circunstancia en la que los profesores necesitaran conocer los datos de los padres de los alumnos, como podría ser ante situaciones de riesgo, y no dispusieran de ellos, estarían igualmente habilitados para recabarlos de los alumnos.

Centros educativos y el acceso al contenido de dispositivos electrónicos de los alumnos, como los sistemas de mensajería instantánea (WhatsApp) o redes sociales

Dada la información que se contiene en los dispositivos con acceso a internet, así como la trazabilidad que se puede realizar de la navegación efectuada por los usuarios, el acceso al contenido de estos dispositivos de los alumnos, incluyendo su clave, supone un acceso a datos de carácter personal que requiere el consentimiento de los interesados o de sus padres o tutores si se trata de menores.

No obstante, cuando se ponga en riesgo la integridad de algún alumno (situaciones de ciberacoso, sexting, grooming, violencia de género o la comisión de un delito), el centro educativo podría, previa autorización de la autoridad competente en la materia, acceder a dichos contenidos sin el consentimiento de los interesados.

Educación continua a través de redes sociales o plataformas.

Actualmente las actividades educativas se han desarrollado en plataformas digitales con la finalidad de dar continuidad en medida de lo posible a las actividades de aprendizaje, lo anterior derivado de la implementación del confinamiento para evitar la propagación de la pandemia provocada por el virus SARS-CoV-2.

Lo anterior reveló el desconocimiento generalizado del derecho de protección de datos personales, incrementando el uso de datos personales en internet a través de las diferentes plataformas o aplicaciones sin la debida cautela.

Creación de grupos con aplicaciones de mensajería instantánea entre alumnos y maestros

Con carácter general, las comunicaciones entre los profesores y los alumnos deben tener lugar dentro del ámbito de la función educativa y no llevarse a cabo a través de aplicaciones de mensajería instantánea. Si fuera preciso establecer canales específicos de comunicación, deberían emplearse los medios y herramientas establecidas por el centro educativo y puestas a disposición de alumnos y profesores (por ejemplo, áreas específicas en la intranet del centro o uso de plataformas que cumplan los requisitos que se verán más adelante) o por medio del correo electrónico.

En situaciones concretas, como la realización de una tarea o trabajo específico, por ejemplo con motivo de la participación en un concurso escolar, o de refuerzo que fueran necesarias, se podrían crear con carácter excepcional, siendo aconsejable la participación en el grupo de un tercero, padre o madre de los alumnos.

Creación de grupos con aplicaciones de mensajería instantánea para que sean miembros los padres de los alumnos de su clase

Como cuestión previa, y como sucede en el caso anterior, las comunicaciones entre los profesores y los padres de los alumnos deben llevarse a cabo a través de los medios puestos a disposición de ambos por el centro educativo. Excepcionalmente, y siempre que se contase con el consentimiento de los padres, sería posible la creación de estos grupos, de los que sólo formarían parte los padres que hubieran consentido a ello.

Como excepción, pueden darse supuestos en que sean los propios padres quienes soliciten la creación de un grupo con los profesores dadas las especiales circunstancias del alumno (por ejemplo, requerir necesidades especiales o como consecuencia de su estado de salud). En estos casos sería posible la creación del grupo. En todo caso, sería preferible que los grupos fueran gestionados por los propios padres y la incorporación al grupo no dependiera directamente de los profesores.

Consulta aquí las recomendaciones para el uso de chat institucional
http://itaigro.org.mx/wp-content/uploads/2018/12/Manual-de-configuracion-ITAIGro.pdf

Grabación de imágenes de los alumnos y difusión a través de aplicaciones de mensajería instantánea a los padres

Como parte del ejercicio de la función educativa de la que es responsable el centro docente no se recomiendan estas grabaciones. No obstante, en aquellos casos en los que el interés superior del menor estuviera comprometido, como en caso de accidentes o indisposiciones en una excursión escolar, y con la finalidad de informar y tranquilizar a los padres, titulares de la patria potestad, se podrían captar las imágenes y enviárselas. También podría ser posible en los grupos generados a través de aplicaciones de mensajería instantánea relacionados con la específica situación del alumno, a los que se ha hecho referencia en la pregunta anterior.

Se recomienda el envió de imágenes de manera particular, para evitar la difusión de imágenes a terceros no competentes para su conocimiento.

Plataformas de comunicación virtual para la continuidad de clases

Las actividades deben realizarse bajo los principios y deberes anteriormente citados, los docentes procuraran privilegiar en todo momento el interés superior de los menores, por su parte los padres de familia o tutores actuaran de manera responsable y salvaguardando en medida de lo posible su derecho a la intimidad personal y familiar.

Para el caso de entrega de evidencias de cumplimiento a las actividades escolares realizadas en casa, los centros escolares, responsable, docentes y padres de familia o tutores deberán utilizar las herramientas para la configuración de la privacidad y reducir a medida de lo posible la exposición de menores ante todos los integrantes del grupo.

Consulta aquí las recomendaciones para la protección de datos personales en clases virtuales http://itaigro.org.mx/wp-content/uploads/2020/05/Clases-virtuales.jpeg

4.2 Tratamiento de los datos de estudiantes

Publicación de datos

En el ejercicio de la función que tienen asignada los centros educativos han de dar publicidad a información personal derivada de diversas acciones o actividades para las que les legitima la Ley.

Publicidad a las listas de alumnos admitidos

La publicidad de la lista de admisión se puede realizar con la finalidad de informar sobre los alumnos que han sido admitidos en la medida en que la admisión se realiza mediante un procedimiento de concurrencia competitiva en el que se valoran y puntúan determinadas circunstancias.

No obstante, la publicidad deberá realizarse de manera que no suponga un acceso indiscriminado a la información, por ejemplo, publicando la relación de alumnos

admitidos en los tablones de anuncios en el interior del centro o en una página web de acceso restringido a quienes hayan solicitado la admisión.

Esta publicación deberá recoger sólo el resultado final de la lista, no resultados parciales que puedan responder a datos o información sensible o poner de manifiesto la capacidad económica de la familia. Esta información, no obstante, estará disponible para los interesados que ejerciten su derecho a reclamar.

Cuando ya no sean necesarios estos listados, hay que retirarlos, sin perjuicio de su conservación por el centro a fin de atender las reclamaciones que pudieran plantearse.

En caso de situaciones de violencia de género, ¿se puede oponer un alumno a la publicación de su admisión en los listados de un centro educativo?

En estos casos, la norma específica sobre medidas de protección integral de violencia de género establece que en actuaciones y procedimientos relacionados con la violencia de género se protegerá la intimidad de las víctimas; en especial, sus datos personales, los de sus descendientes y los de cualquier otra persona que esté bajo su guarda o custodia. En consecuencia, los centros educativos deberán proceder con especial cautela a tratar los datos de los menores que se vean afectados por estas situaciones.

El alumno se puede oponer a la publicación de su admisión en un centro educativo si se alegan motivos fundamentados y legítimos relativos a su concreta situación personal, como, por ejemplo, razones de seguridad por ser víctima de violencia de género o sufrir algún tipo de amenaza, etc. El centro educativo lo tiene que excluir del listado de admitidos que se publique.

Publicidad en los centros colocando anuncios en las puertas de las aulas la relación de alumnos por clases y/o actividades

Para la organización de la actividad docente los centros distribuyen al inicio de cada curso a los alumnos por clases, materias, actividades y servicios.

Para dar a conocer a los alumnos y a sus padres o tutores esta distribución, se pueden colocar dichas relaciones en los tablones de anuncios o en las entradas de las aulas, durante un tiempo razonable para permitir el conocimiento por todos los interesados.

Si el centro educativo utiliza una plataforma para la gestión educativa, se recomienda que cada alumno, sus padres o tutores accedan a dicha información mediante el uso de una identificación de usuario y su correspondiente contraseña.

Profesores en prácticas y la utilización de datos personales de los alumnos para trabajos propios universitarios

En la medida que no se estarían tratando los datos para la educación de los alumnos, sino para otra finalidad como la formación de los profesores, resulta aconsejable que procedan a disociar los datos de manera que no se puedan identificar a los alumnos. De lo contrario, tendrán que contar con su consentimiento o el de sus padres o tutores.

Calificaciones

Publicación de las calificaciones escolares

Las calificaciones de los alumnos se han de facilitar a los propios alumnos y a sus padres.

En el caso de comunicar las calificaciones a través de plataformas educativas, éstas sólo deberán estar accesibles para los propios alumnos, sus padres o tutores, sin que puedan tener acceso a las mismas personas distintas.

No obstante, sí sería posible comunicar la situación del alumno en el entorno de su clase, por ejemplo, citando su calificación frente a sus compañeros.

Entrega de calificaciones oralmente en clase

No existe una regulación respecto de la forma de comunicar las calificaciones. Aunque sería preferible que las calificaciones se notificarán en la forma indicada en el punto anterior, sería posible enunciarlas oralmente, evitando comentarios adicionales que pudieran afectar personalmente al alumno.

Acceso a la información de estudiantes

Los centros educativos disponen de datos de los alumnos de muy diversa naturaleza: identificativos, académicos, familiares, económicos, sociales, de salud, a los que han de acceder sólo las personas que lo necesiten para ejercer la función que tengan encomendada, ya sean del equipo directivo, tutores, profesores, personal de administración o de servicios.

Acceso de los profesores a los expedientes académicos de los alumnos matriculados en el centro educativo

Con carácter general y salvo que exista alguna causa debidamente justificada, el profesor ha de tener acceso al expediente académico de los alumnos a los que imparte la docencia, sin que esté justificado acceder a los expedientes de los demás alumnos del centro.

Acceso a la información de salud de los alumnos

Los profesores han de conocer y, por tanto, acceder a la información de salud de sus alumnos que sea necesaria para la impartición de la docencia, o para garantizar el adecuado cuidado del alumno, por ejemplo, respecto a discapacidades auditivas, físicas o psíquicas, trastornos de atención, TDAH o enfermedades crónicas.

Igualmente, han de conocer la información relativa a las alergias, intolerancias alimentarias o la medicación que pudieran requerir para poder prestar el adecuado cuidado al alumno tanto en el propio centro como con ocasión de actividades fuera del centro, como visitas, excursiones o convivencias guiadas por profesores.

Acceso de los padres a la información sobre las ausencias escolares de sus hijos

Si los padres, como sujetos que ostentan la patria potestad, entre cuyas obligaciones está la de educarlos y procurarles una formación integral, tienen acceso a la información sobre la ausencia escolar de sus hijos.

Información escolar de los alumnos a sus familiares

La información escolar se proporcionará solo a los padres que ostenten la patria potestad o a los tutores, nunca a otros familiares, salvo que estuvieren autorizados por aquellos y constase claramente esa autorización.

Acceso a la información académica por padres separados

En los supuestos de patria potestad compartida, con independencia de quién tenga la custodia, ambos progenitores tienen derecho a recibir la misma información sobre las circunstancias que concurran en el proceso educativo del menor, lo que obliga a los centros a garantizar la duplicidad de la información relativa al proceso educativo de sus hijos, salvo que se aporte una resolución judicial que establezca la privación de la patria potestad a alguno de los progenitores o algún tipo de medida penal de prohibición de comunicación con el menor o su familia.

En caso de conflicto entre los progenitores sobre el acceso a la información académica de sus hijos, deberá plantearse ante la autoridad competente.

Transferencias de los datos de los alumnos

Como regla general las transferencias, ya sean nacionales o internacionales, se encuentran sujetas al consentimiento del titular de los datos, salvo la actualización de las excepciones previstas en las normas aplicables.

Los centros educativos reciben peticiones de otros centros, instituciones y organismos de otras administraciones e incluso de entidades privadas para que se les facilite información personal de los alumnos, por ejemplo de los servicios sociales, o de la autoridad sanitaria.

La comunicación de datos requiere, con carácter general, el consentimiento de los interesados, de los alumnos o de sus padres o tutores, salvo que esté legitimada por otras circunstancias, como que permita u obligue a ella una Ley, por ejemplo para solucionar una urgencia médica, o se produzca en el marco de una relación jurídica aceptada libremente por ambas partes, por ejemplo, la establecida entre los padres y el centro al matricular a sus hijos.

En estos supuestos se pueden comunicar los datos sin necesidad de obtener el consentimiento de los afectados.

Comunicación de datos de estudiantes

Facilitación de datos de los alumnos a otros centros educativos

En caso de transferencia, la comunicación de datos al nuevo centro educativo en el que se matricule el alumno sin necesidad de recabar su consentimiento o el de sus padres o tutores.

Centros educativos situados en otros países para intercambios de alumnos o estancias temporales

Dado que el acceso a los datos del alumno sería necesario para que el centro en el que se vaya a desarrollar el intercambio pueda realizar adecuadamente su función educativa, teniendo en cuenta que la participación del alumno en el programa deberá haber contado con la solicitud o autorización de los titulares de la patria potestad. La comunicación responderá al adecuado desarrollo de la relación jurídica solicitada por los propios representantes legales del alumno.

La transmisión deberá limitarse a los datos que resulten necesarios para el adecuado desarrollo de esa acción educativa y para el cuidado del menor que el centro de destino pudiera requerir.

Cuando el centro destinatario de los datos se encuentre en un país fuera del Estado Mexicano, la comunicación constituye una transferencia internacional de datos.

Autoridades Educativas

Los centros educativos públicos, comunicarán los datos personales de los alumnos necesarios para el ejercicio de las competencias que tienen atribuidas las autoridades educativas como, por ejemplo, la expedición de títulos.

Comunicación de datos a las Autoridades de Seguridad Pública

Las comunicaciones de datos a las autoridades de seguridad pública son obligatorias siempre que sean necesarios para la prevención de un delito o para la sanción de la comisión de un delito.

En todo caso, la petición que realicen las autoridades de seguridad pública, en el ejercicio de sus competencias, debe ser concreta, específica y motivada, de manera que no haya una comunicación de datos indiscriminada.

Aunque se cumplan los requisitos para la comunicación de datos a las autoridades de seguridad pública, es aconsejable que el centro documente la comunicación de los datos.

Comunicación de datos a los Servicios Sociales

Siempre que sea para la determinación o tratamiento de situaciones de riesgo o desamparo competencia de los servicios sociales. La comunicación estaría amparada en el interés superior del menor, recogido en la Ley General de los Derechos de Niñas, Niños y Adolescentes y la Ley General de Prestaciones de Servicios para la Atención, Cuidado y Desarrollo Infantil. En estos supuestos no se necesita el consentimiento de los interesados.

Comunicación de datos a las instituciones sanitarias

Se pueden facilitar los datos sin consentimiento de los interesados a los centros sanitarios cuando el motivo sea la **prevención o el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos**, o la gestión de servicios sanitarios, siempre que se realicen por profesionales sanitarios sujetos al secreto profesional o por otras personas sujetas a la misma obligación.

Por ejemplo, cuando sea precisa la asistencia sanitaria a un alumno que se haya accidentado, indispuesto o intoxicado con la alimentación o bien para la prevención y salvaguarda del derecho a la salud de terceros.

Solicitud del centro educativo de acceso a información sobre la asistencia sanitaria prestada

En caso de que fuera necesario, el centro educativo puede solicitar la información referente a la prestación del servicio para abonar en la asistencia sanitaria en los supuestos en los que la misma se encontrara cubierta por el seguro de responsabilidad civil que hubiera suscrito el centro para responder de las lesiones causadas como consecuencia del normal desarrollo de la actividad escolar.

Comunicación de datos a los Servicios Sanitarios como campañas de vacunación o programas de salud escolar dentales o alimentarios

Se pueden facilitar los datos de los alumnos a los servicios de salud que los requieran sin necesidad de disponer del consentimiento de los interesados en respuesta a una petición de las autoridades sanitarias cuando sean estrictamente necesarios para garantizar la salud pública o si tiene por finalidad la realización de actuaciones de salud pública que tengan encomendadas.

Por ejemplo, ante un caso de infección en un centro educativo, para la realización de estudios que permitan descartar la presencia de la enfermedad en el entorno del centro educativo.

Comunicación de datos a instituciones, entidades o empresas que van a ser visitadas por los alumnos en una actividad extraescolar, por ejemplo, una exposición, un museo, una fábrica o un club deportivo

Se debe contar con el consentimiento previo e inequívoco de los interesados o de sus padres o tutores, cuando los datos sean comunicados para las finalidades

propias del teatro, museo, exposición o de la fábrica, por ejemplo, el control de entrada o para sus programaciones futuras.

La información que sobre estos eventos se facilita a los padres para su autorización debe incluir la relativa a la comunicación de datos a estas entidades, así como la propia autorización. La comunicación, en caso de ser autorizada, implicaría la posibilidad del tratamiento de los datos exclusivamente para los fines que se han indicado, al ser ésta necesaria para que el alumno pueda participar en esa actividad.

Comunicación de datos de los alumnos y de sus padres y madres a las Asociaciones de Padres de Familia

No sin el previo consentimiento de los interesados. Las Asociaciones de Padres de Familia son responsables del tratamiento de los datos de carácter personal que hayan recabado, debiendo cumplir con la normativa de protección de datos aplicable en su tratamiento.

Tratamiento de imágenes de estudiantes

Proteger la privacidad y los datos personales de los menores es de vital importancia, hoy en día el desarrollo trepidante de las TIC´s (Tecnologías de la Información y la comunicación), rebasan considerablemente la cultura de la protección de datos personales existente, por lo que realizar actividades de recolección y difusión de imágenes se ha convertido en algo cotidiano para cualquier persona con acceso a un móvil con cámara.

Con frecuencia durante las celebraciones de actos escolares o de eventos en centros educativos en los que los alumnos y los profesores son participes, familiares y el propio centro toman fotografías y graban vídeos en los que se recolectan sus imágenes. Estos hechos, comunes en los eventos escolares, dan lugar a que se planteen muchas cuestiones sobre quién y cómo se pueden captar las imágenes, qué requisitos se han de cumplir, con qué finalidad y a quién se pueden comunicar.

Según quién vaya a grabar las imágenes y la finalidad para la que se graben será necesario observar unos determinados requisitos.

Si la grabación de las imágenes se produjera por el centro escolar con fines educativos, como trabajos escolares o evaluaciones, el centro o el responsable estarían legitimados para dicho tratamiento sin necesidad del consentimiento de los alumnos o de sus padres o tutores. Cuando la grabación de las imágenes no corresponda con dicha función educativa, sino que se trate de imágenes de acontecimientos o eventos que se graban habitualmente con fines de difusión en la revista escolar o en la web del centro, se necesitará contar con el consentimiento de los interesados, a quienes se habrá tenido que informar con anterioridad de la finalidad de la grabación, en especial de si las imágenes van a estar accesibles de manera indiscriminada o limitada a la comunidad escolar.

En caso de conflicto entre los progenitores sobre la grabación de las imágenes de sus hijos, deberá plantearse ante el juez y demás autoridades competentes en la materia para su resolución.

Se recomienda que la publicación en la web de los centros tenga lugar en un espacio privado, al que se acceda mediante identificación y contraseña.

Te invitamos a consultar las recomendaciones emitidas en la materia:

http://itaigro.org.mx/wp-content/uploads/2019/04/Recomendaciones-imagen-sujetos-obligados.png

http://itaigro.org.mx/wp-content/uploads/2019/04/Recomendaciones-imagen-sujetos-obligados.png

Consulta aquí la Guía para la configuración de la privacidad en redes sociales
http://itaigro.org.mx/wp-content/uploads/2018/12/Manual-de-configuracion-ITAIGro.pdf

Grabación de imágenes de actividades docentes

Los centros educativos y la captación de imágenes de los alumnos durante las actividades escolares

Cabe distinguir entre la toma de imágenes como parte de la función educativa, en cuyo caso los centros estarían legitimados para ello, de las grabaciones que no responderían a dicha función, por ejemplo, la difusión del centro y de sus actividades, para lo que se deberá disponer del consentimiento de los interesados o de sus padres o tutores.

También sería posible la toma de imágenes de los alumnos en determinados eventos desarrollados en el entorno escolar para la única finalidad de que los padres pudieran tener acceso a ellas. Este acceso a las imágenes debería siempre llevarse a cabo en un entorno seguro que exigiera la previa identificación y autenticación de los alumnos, padres o tutores (por ejemplo, en un área restringida de la intranet del centro), limitándose a las imágenes correspondientes a eventos en los que el alumno concreto hubiera participado. En todo caso, sería preciso recordar a quienes acceden a las imágenes que no pueden, a su vez, proceder a su divulgación de forma abierta.

Grabación de imágenes de los alumnos para una actividad escolar

Los profesores, en el desarrollo de la programación y enseñanza de las áreas, materias y módulos que tengan encomendados, pueden disponer la realización de ejercicios que impliquen la grabación de imágenes, normalmente de los propios alumnos, que sólo deberán estar accesibles para los alumnos involucrados en dicha actividad, sus padres o tutores y el profesor correspondiente.

En ningún caso el hecho de realizar la grabación supone que la misma se pueda difundir de forma abierta en internet y que se pueda acceder de manera indiscriminada.

En estos casos el responsable del tratamiento es el propio centro educativo o el responsable.

Grabación de imágenes de actividades desarrolladas fuera del centro escolar

La grabación de imágenes fuera del recinto escolar por los centros requiere el consentimiento de los interesados, o de sus padres o tutores, siempre que no se realice en ejercicio de la función educativa.

Si la grabación se realiza por terceros, por ejemplo, por los responsables de la empresa, museo, exposición o club deportivo que se esté visitando, o en el que se desarrolle una actividad deportiva, será obligación de estos terceros disponer del consentimiento de los interesados que habrán podido recabar a través del centro.

4.3 Tratamiento de datos en internet

Utilización de plataformas educativas

La utilización de plataformas educativas, tanto de gestión como de aprendizaje o entornos virtuales de aprendizaje, son cada vez más usuales y la recolección de datos personales de manera indiscriminada, por lo que se genera la necesidad de dar a conocer las medidas básicas para el cumplimiento de la salvaguarda del derecho humano de protección de datos personales.

Responsable del tratamiento de los datos personales de los alumnos en las plataformas educativas

Los centros o los sujetos obligados, son los responsables del tratamiento de los datos personales utilizados en las plataformas educativas, ya que son los que suscriben el contrato de prestación de servicios con las empresas titulares de las plataformas educativas, que actúan como ***encargadas*** del tratamiento.

Actuar de los centros educativos si prestan el servicio de adquisición de libros digitales de forma centralizada

Cuando la adquisición implique la remisión de la relación de los alumnos con datos personales a las editoriales, se deberá informar de dicha comunicación de datos y de las finalidades de la comunicación a los alumnos y/o a los padres o tutores.

Tratamiento de los datos personales por parte de las editoriales

Las editoriales carecen de legitimación para el tratamiento de los datos personales para fines distintos de los previstos en la licencia del servicio (resultado de pruebas, perfiles, publicidad, etc.), por lo que tendrán que recabar el consentimiento específico.

Utilización de herramientas de almacenamiento en nubes distintas de las plataformas educativas

Sólo si reúnen las garantías previstas en la normativa de protección de datos. En tal caso deberán establecer unas normas que garanticen el adecuado tratamiento de los datos personales.

La utilización de aplicaciones por los profesores en dispositivos personales (tableta, móvil, etc.) debe garantizar la política de privacidad definida por el centro o el responsable con las garantías establecidas en la normativa de protección de datos.

En particular, es de especial importancia que el uso de esas aplicaciones no implique una transmisión de los datos de los alumnos al prestador del servicio contratado para que los utilice para sus propios fines o los almacene de forma permanente, incluso con posterioridad a la terminación del contrato o cuando el alumno ya no curse estudios en el centro educativo. Tampoco debería implicar la renuncia del centro educativo al acceso a los datos o a su supresión.

Computo en la nube

Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:

I. Cumpla, al menos, con lo siguiente:

- **a.** Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la LGPDPPSO y demás normativa aplicable;
- **b.** Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;
- **c.** 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, y
- **d.** Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio;

II. Cuente con mecanismos, al menos, para:

- **a)** Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
- **b)** Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
- **c)** Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio;

d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos, y
e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales, conforme a la LGPDPPSO y demás disposiciones que resulten aplicables en la materia.

Medidas que deberán adoptar los centros o los responsables en relación con la seguridad de los datos

En relación con las obligaciones del encargado del tratamiento las obligaciones para éste último, de forma específica, podemos precisar que la normatividad de datos personales señala como obligaciones del encargado del tratamiento las siguientes:

a) Dependencia: únicamente puede tratar los datos conforme a las instrucciones que le facilite el responsable.
b) Finalidad: debe abstenerse de tratar los datos para finalidades distintas a las instruidas por el responsable.
c) Seguridad: debe cumplir con las medidas de seguridad previstas en la normatividad de datos personales.
d) Confidencialidad: debe mantener la confidencialidad sobre los datos que trate y esta obligación subsistirá aún después de la finalización del contrato de prestación de servicios que le vincula al responsable.
e) Cancelación: una vez finalizada la relación, o siempre que el responsable se lo pida, debe suprimir los datos personales que trate, salvo una ley exija su conservación.
f) No transmisión: no podrá transferir ni remitir los datos a terceros, salvo que:
    1. El responsable le dé instrucciones para que lo haga.
    2. El responsable le permita específicamente subcontratar.
    3. Los requiera la autoridad competente en términos de LGPDPPSO.

Al finalizar el contrato de prestación de servicios

Los centros educativos deben tener la opción de exigir al encargado del tratamiento la portabilidad de la información a sus propios sistemas, o a otro nuevo encargado de tratamiento, con garantías de la integridad de la información.

A tal efecto el responsable debe obtener información respecto a la manera de recuperar los datos, de forma que quede garantizada contractualmente la portabilidad.

Al finalizar la contratación, el encargado del tratamiento tiene que garantizar al responsable del tratamiento el borrado seguro de los datos personales donde se encuentren alojados, de tal forma que se impida su reutilización. Además, deberá asegurar el bloqueo o borrado de todos los usuarios para imposibilitar el acceso a la plataforma educativa.

Se considera una buena práctica que a la finalización del contrato se asegure la destrucción o devolución de los datos con un certificado de destrucción o con un acuse de recibo.

Publicación de datos en la web de los centros educativos

Las páginas web de los centros educativos o los responsables contienen información referida a sus características, su organización, las materias que imparte, las actividades que desarrolla, los servicios que ofrece, las relaciones con otros centros, para lo que en ocasiones incluyen información de carácter personal sobre la dirección, el profesorado y los alumnos.

Publicación en las páginas web del centro educativo los datos de los profesores, tutores y otros responsables del centro

De acuerdo a la situación en específico:

- Si se trata de una página web abierta, sería necesario contar con su consentimiento previo dado que se trata de una comunicación de datos a los que puede acceder cualquier persona de manera indiscriminada y no resulta necesaria para el ejercicio de la función educativa encomendada a los centros.
- Si la información está restringida a los alumnos del centro y a sus padres o tutores se puede publicar, debiendo informar a los docentes y, en caso de incluir la dirección de correo electrónico para contacto, que sea la del centro y no las personales que tengan los profesores en el ámbito educativo.

Publicación en la página web del centro información relativa a los alumnos, como fotografías o vídeos

Siempre que se disponga del consentimiento de los alumnos o de sus padres o tutores. También podría llevarse a cabo de manera que no se pudiera identificar a los alumnos, por ejemplo, **pixelando las imágenes**.

También sería posible su publicación cuando responda a determinados eventos desarrollados en el entorno escolar con la única finalidad de que los padres pudieran tener acceso a ella. Este acceso debería llevarse a cabo siempre en un entorno seguro que exigiera la previa identificación y autenticación de los alumnos, padres o tutores (por ejemplo, en un área restringida de la intranet del centro), limitándose a la información correspondiente a eventos en los que el alumno concreto hubiera

participado. En todo caso, sería preciso recordar a quienes acceden a la información que no pueden, a su vez, proceder a su divulgación de forma abierta.

Publicación de datos en redes sociales

La publicación de datos personales en redes sociales por parte de los centros educativos requiere contar con el consentimiento de los interesados, a los que habrá que informar previamente de manera clara de los datos que se van a publicar, en qué redes sociales, con qué finalidad, quién puede acceder a los datos, así como de la posibilidad de ejercer sus derechos de acceso, rectificación, cancelación y oposición.

Se entenderá el consentimiento como una manifestación de voluntad libre, específica, informada e inequívoca, mediante declaración o clara acción afirmativa.

4.4 Otros supuestos

4.4.1 Videovigilancia

La recolección de imágenes en los centros educativos a través de sistemas de videovigilancia con el objetivo de mantener la seguridad e integridad de personas y las instalaciones, ha de observar la normativa de protección de datos personales, en la medida que implica el tratamiento de los datos de alumnos, profesores, familiares, etc.

Instalación de cámaras de videovigilancia

No es recomendable utilizar las cámaras en todas las instalaciones. Dada la intromisión que supone en la intimidad de las personas, tanto de los alumnos como de profesores y demás personas cuya imagen puede ser captada por las cámaras, los sistemas de videovigilancia no podrán instalarse en vestidores, sanitarios o zonas de descanso de personal docente o de otros trabajadores.

Cámaras de videovigilancia en las aulas

Resultaría desproporcionado, pues durante las clases ya está presente un profesor. Cabría la posibilidad de que, fuera del horario laboral y en los supuestos de desocupación de las aulas, se pudieran activar mecanismos de videovigilancia con la finalidad de evitar daños en las instalaciones y materiales.

Instalación de cámaras de videovigilancia en los patios de recreo y comedores.

Deberá considerarse si la instalación responde a la protección del interés superior del menor, toda vez que, sin perjuicio de otras actuaciones como el control presencial por adultos, se trata de espacios en los que se pueden producir acciones que pongan en riesgo su integridad física, psicológica y emocional.

Importancia de informar de la existencia de un sistema de videovigilancia

El principio de información establece la obligación de informar a los titulares sobre la recolección, uso y transferencia de los datos personales, en este caso la imagen, por lo que se recomienda colocar un anuncio en lugar suficientemente visible en aquellos espacios donde se hayan instalado las cámaras.

Adicionalmente también se deberá disponer de un aviso de privacidad integral que incluya todos los aspectos requeridos por la normativa aplicable.

5. DERECHO DE PROTECCIÓN DE DATOS PERSONALES

En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen.

Los derechos ARCO son una garantía del derecho de autodeterminación de las personas como titulares de datos personales que les permite mantener el control y disponer de sus datos personales frente a los responsables pertenecientes al sector público y al privado.

Los derechos ARCO son personalísimos por lo que por regla general, únicamente pueden ejercerse por la persona a quien le conciernen los datos personales, ya sea directamente o a través de un representante. Para el ejercicio de los derechos ARCO es necesario que el titular de los datos personales acredite su identidad, así como, de ser el caso, la identidad y personalidad de su representante.

Generalidades

Acceso

El derecho de acceso es el “derecho de acceder a sus datos personales que obren en posesión del responsable, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento”.

Por ejemplo: el tipo de datos que trata, las finalidades del tratamiento, las personas que intervienen en el tratamiento, la existencia de encargados, la existencia de transferencias, los destinatarios de las transferencias, las finalidades de las transferencias y los datos transferidos, entre otra información que el titular esté interesado en conocer.

Gran parte de esa información debe darse a conocer al titular desde el aviso de privacidad en cumplimiento del principio de información.

Rectificación

El titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados.

El derecho de rectificación tiene una estrecha relación con el principio de calidad de los datos personales. El principio de calidad se cumple cuando los datos personales tratados son exactos, completos, pertinentes, correctos y actualizados. En aquellos casos en que el titular proporciona directamente sus datos, se considera que los mismos cumplen con el principio de calidad, hasta en tanto el titular manifieste y acredite lo contrario o el responsable cuente con evidencia objetiva que lo contradiga.

Cancelación

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.

De conformidad con lo dispuesto por la LGPDPPSO, la cancelación de los datos personales no se lleva a cabo de forma inmediata, sino que en muchos casos debe ser precedida por un periodo de bloqueo. El responsable de los datos personales debe establecer y documentar los procedimientos para la conservación, bloqueo —y en su caso— supresión de los datos personales.

Oposición

El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando:

I. Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular, y

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

El derecho de oposición no es absoluto. La solicitud de oposición no procederá cuando, entre otras causas, los datos personales sean necesarios para las finalidades esenciales de la relación jurídica entre las partes, como por ejemplo, el cumplimiento de una obligación contractual o una disposición legal.

De resultar procedente el derecho de oposición, el responsable no podrá tratar los datos personales sobre los que el titular haya ejercido ese derecho para las finalidades que el titular haya especificado. Lo anterior, sin afectar el tratamiento de los datos personales por parte del responsable para las demás finalidades previstas en el aviso de privacidad que no hayan sido objetadas.

Acreditación

La identidad del titular se puede acreditar de las siguientes maneras:

I. presentando copia de su documento de identificación habiendo exhibido el original para su cotejo,

II. a través de instrumentos electrónicos por los cuales sea posible identificarlo fehacientemente o

III. a través de otros mecanismos de autenticación permitidos por las disposiciones legales o que hayan sido establecidos por el responsable. En caso de que el titular utilice su firma electrónica avanzada o el instrumento electrónico que la sustituya, no será necesario que presente alguna otra identificación.

Si la solicitud se presenta a través de un **representante legal**, éste tendrá la obligación de acreditar:

I. la identidad del titular,

II. su identidad y

III. el mandato que se le ha otorgado mediante instrumento público, carta poder firmada ante dos testigos o la declaración en comparecencia personal del titular.

El ejercicio de los derechos ARCO por parte **de menores de edad** y personas en estado de interdicción o incapacidad debe realizarse teniendo en cuenta las reglas de representación previstas en la legislación civil y la demás que resulte aplicable.

5.1 Derecho de Acceso

Obligación de las instituciones educativas o el responsable de responder a una solicitud de derecho de acceso

El plazo para responder a las solicitudes ARCO: la respuesta a la solicitud ARCO deberá ser comunicada al titular o a su representante, en un plazo no mayor a 20 días hábiles contados a partir de la recepción de la solicitud según la normativa del sector privado y contados a partir del día siguiente a la recepción de la solicitud conforme a la LGPDPPSO, con posibilidad de prorrogar el plazo por 10 días hábiles, es decir, la mitad de la duración del plazo original.

5.2 Derecho de rectificación

Solicitud de rectificación de los datos de su expediente escolar

Se puede solicitar la rectificación, siempre que se constate un error. El centro educativo o el responsable tendrán que corregirlo siempre que se acredite el error. Se podrá ejercitar tantas veces como se adviertan. Si se trata de menores de edad, lo tienen que ejercer sus padres o tutores.

Este derecho de rectificación no se aplica a las calificaciones o al contenido de los informes del expediente escolar que se rigen por su normativa específica.

Procedencia del derecho de rectificación para modificar un informe de evaluación psicopedagógica

El derecho de rectificación se refiere a modificar los datos de carácter personal que sean inexactos o incompletos (por ejemplo, el cambio de dirección postal), pero no se puede utilizar para tratar de modificar la opinión realizada por un profesional a través del correspondiente informe que se rige por su normativa específica.

5.3 Derecho de cancelación

Procedencia de la cancelación de la información de los expedientes académicos a solicitud de los alumnos, de sus padres o tutores en las instituciones educativas

Sin perjuicio de lo establecido en las normas archivísticas y de educación aplicable, la información de los expedientes académicos requiere su conservación en la medida en que puede ser solicitada por los alumnos después de finalizados los estudios.

Datos de salud obtenidos por el Equipo de Orientación Educativa

Se suprimirán sus datos personales cuando no sean necesarios para el desarrollo de la función educativa y, en su caso, al finalizar la escolarización del alumno en el centro, por ejemplo, los datos sobre las alergias alimentarias, es decir una vez que la finalidad ya fue cumplida.

5. 4 Derecho de oposición

Oposición de los alumnos o los familiares a la publicidad de sus datos

Puede existir un motivo legítimo y fundado, referido a una concreta situación personal, para oponerse a la publicidad de su información personal.

Por ejemplo, en los casos en los que se ha acordado por los jueces el alejamiento de uno de los progenitores o se le ha privado de la patria potestad y la publicidad de información personal pueda suponer un riesgo para la integridad física y psíquica del alumno o del otro progenitor.

5.5 Derecho de portabilidad

La LGPDPPSO les reconoce también el derecho de portabilidad de datos personales.

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.

Los Estándares Iberoamericanos reconocen, adicionalmente, el derecho de portabilidad, el derecho de no ser objeto de decisiones individuales automatizadas y el de limitación del tratamiento de los datos personales.

Se recomienda visitar la siguiente dirección electrónica para mayor información

http://itaigro.org.mx/derechos-arco

6. DATOS PERSONALES SENSIBLES

Los datos personales sensibles son definidos por la LGPDPPSO 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 preferencia sexual.*

6.1 Bases de datos que contienen datos personales sensibles

La creación de bases de datos con información personal de carácter sensible se sujeta a reglas legales más estrictas y se encuentra vedada salvo que **existan finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado o bien exista una base concreta de legitimación del tratamiento**.

La LGPDPPSO prohíbe la creación de bases de datos que contengan datos personales sensibles sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el responsable del tratamiento:

El artículo 7 de la LGPDPPSO indica: “Por regla general no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22 de esta Ley”, de esto se desprende entonces, **que la creación de bases de datos personales con información sensible debe estar debidamente justificada por parte del responsable.**

Los centros educativos recaban en muchos casos, a través de sus servicios médicos, datos de salud relacionados con las lesiones o enfermedades que pudieran sufrir los alumnos durante su estancia en el centro. También recogen datos

de salud de los alumnos para el ejercicio de la función educativa, discapacidades físicas o psíquicas, por ejemplo del síndrome TDAH. Para prestar el servicio de comedor también es necesario recabar datos de salud que permitan conocer los alumnos que son diabéticos o que padecen alergias alimentarias. También son datos de salud los contenidos en los informes psicopedagógicos de los alumnos.

6.2 Datos personales relativos a la salud

Los datos relativos a la salud son datos personales de carácter sensible, en tanto que se refieren al estado de salud física o mental de un individuo. Los datos relativos a la salud incluyen la prestación de servicios de atención médica que puede revelar información sobre el estado de salud actual, presente o futuro de su titular.

No obstante, es preciso señalar que en la legislación nacional aplicable a los sectores público y privado no existe una definición concreta de datos relativos a la salud.

Por su parte el Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés), en el apartado 15 de su artículo 4, define a los datos relativos a la salud como “datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud”.

En relación con lo anterior, el considerando 35 del RGPD indica que deben considerarse incluidos los datos relativos al estado de salud del interesado (titular en términos de la normatividad nacional) que dan información sobre su estado de salud física o mental pasado, presente o futuro. De acuerdo con el RGPD, en esta categoría se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia.

Así, el RGPD considera que los datos relativos a la salud pueden incluir un listado amplio:

Todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de ***pruebas o exámenes*** *de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.*

Los datos relativos a la salud son considerados datos personales sensibles, según se dispone en la normatividad de datos personales aplicable, considerando que

estos pueden referirse a la esfera más íntima de su titular o bien su tratamiento ilícito puede implicar un riesgo grave o discriminación para su titular.

Derivado de la naturaleza sensible de los datos relativos a la salud, se considera que estos deben ubicarse bajo un régimen de protección legal especial ya que su utilización no autorizada podría afectar los derechos y libertades fundamentales del titular de los datos personales.

Como se señaló en párrafos anteriores la LGPDPPSO prohíbe la creación de bases de datos que contengan datos personales sensibles. Esta regla se aplica a los datos relativos a la salud, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el responsable del tratamiento. Es decir, si bien todas las bases de datos deben cumplir con una finalidad legítima y concreta, la creación de bases de datos sensibles debe ir acorde con las actividades o fines del tratamiento que persigue el responsable.

Asimismo, de conformidad con la LGPDPPSO, cuando se requiera el consentimiento para el tratamiento de datos personales sensibles, como es el tratamiento de datos relativos a la salud, éste deberá ser expreso y por escrito, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca.

En consecuencia, el tratamiento de datos personales relativos a la salud, además, deberá ser el que resulte necesario, adecuado y relevante en relación con las finalidades que justifiquen su tratamiento y que se encuentren previstas en el aviso de privacidad, el cual deberá señalar explícitamente el tratamiento de estos datos. En especial, frente a éste, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable.

Tratamiento automatizado de datos personales sensibles.

El responsable no podrá llevar a cabo tratamientos automatizados de datos personales que tengan como efecto la **discriminación** de las personas por su origen étnico o racial, **su estado de salud presente, pasado o futuro**, su información genética, sus opiniones políticas, su religión o creencias filosóficas o morales y su preferencia sexual.

7. TRANSFERENCIAS DE DATOS PERSONALES

Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones, por ejemplo cuando se trate de una transferencia nacional entre responsables; cuando se trate de un caso fuera del territorio nacional el tercero receptor o el encargado debe estar obligado a proteger los datos personales conforme a los principios y deberes en materia de protección de datos personales.

Se recomienda observar lo dispuesto en el Titulo Quinto "Comunicaciones de Datos Personales" Capítulo Único de las Transferencias y Remisiones de Datos Personales para mayor información.

8. ELIMINACIÓN DE DATOS PERSONALES

La eliminación segura de datos personales en los diferentes tipos de almacenamiento debe llevar un proceso seguro, una vez que los datos personales han cumplido con las finalidades para las que fueron recabados y sin contravención a la legislación archivística aplicable.

Bloqueo

La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;

Supresión de datos personales

El responsable deberá suprimir los datos personales en su posesión cuando hayan dejado de ser necesarios para el cumplimiento de las **finalidades concretas, explícitas, lícitas y legítimas** que motivaron su tratamiento, **previo bloqueo** en su caso, y una vez que concluya el **plazo de conservación** de los mismos. En la supresión de los datos personales, el responsable deberá implementar métodos y técnicas orientadas a la **eliminación definitiva** de éstos.

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

Supresión de datos personales por parte de terceros.

Cuando sea procedente el ejercicio del derecho de cancelación, el responsable deberá adoptar todas aquellas medidas razonables para que los datos personales sean suprimidos también por los terceros a quienes se los hubiere transferido.

8.1 Anonimización

De acuerdo con la AEPD, la finalidad del proceso de anonimización es eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales.

8.2 Disociación

Señalado por la LGPDPPSO como aquel procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

Los datos personales son sujetos un proceso de disociación, de tal manera que no puedan asociarse al titular ni permitir la identificación del mismo, salvo aquellos datos personales que por medio de un procedimiento posterior se puedan asociar de nuevo al titular.

8.3 Seudonimización

El RGPD lo define como: “El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable”.

9. ANEXOS

Marco normativo básico

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

http://itaigro.org.mx/wp-content/uploads/2017/12/LEYGENERALDEPROTECCIONDEDATOSPERSONALES.pdf

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

http://itaigro.org.mx/wp-content/uploads/2018/07/LINEAMIENTOS-PORTABILIDAD.pdf

Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal.

http://dof.gob.mx/nota_detalle.php?codigo=5511114&fecha=23/01/2018

Lineamientos que establecen los Parámetros, Modalidades y Procedimientos para la Portabilidad de Datos Personales.

http://itaigro.org.mx/wp-content/uploads/2018/07/LINEAMIENTOS-PORTABILIDAD.pdf

Ley número 466 de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Guerrero.

http://itaigro.org.mx/wp-content/uploads/2017/12/LEYDEPROTECCIONDEDATOSPERSONALES.pdf

Materiales y recursos útiles en materia de protección de datos personales

Recomendaciones para tutelar el derecho a la intimidad de niñas, niños y adolescentes a través de la protección de datos personales.

http://itaigro.org.mx/wp-content/uploads/2019/04/Recomendaciones-imagen-sujetos-obligados.png

Recomendaciones para garantizar el derecho a la privacidad de la imagen de niñas, niños y adolescentes en las actividades festivas en conmemoración al día del niño y de la niña.

http://itaigro.org.mx/wp-content/uploads/2019/04/Recomendaciones-imagen-empresas.png

Recomendaciones para la protección de datos personales en clases virtuales

http://itaigro.org.mx/wp-content/uploads/2020/05/Clases-virtuales.jpeg

Manual de configuración de privacidad en redes sociales

http://itaigro.org.mx/wp-content/uploads/2018/12/Manual-de-configuracion-ITAIGro.pdf

Recomendación de chat institucional

https://www.youtube.com/watch?v=LQrVbNSyBDY#action=share

Derechos ARCO

http://itaigro.org.mx/derechos-arco/

https://youtu.be/_pZbCwA7EWo

Fuentes

Convenio N° 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y a su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos.

http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf

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

http://itaigro.org.mx/wp-content/uploads/2017/12/LEYGENERALDEPROTECCIONDEDATOSPERSONALES.pdf

Diccionario de Protección de Datos Personales

file:///C:/Users/Protecci%C3%B3n%20de%20Datos/Downloads/Diccionario%20de%20Datos%20Personales%20_.pdf

Guía para centros educativos

file:///E:/USB%20BLANCA/Dirección%20PDP%202020/Acuerdos%202020/GuiaCentrosEducativos.pdf

La presente guía es una herramienta de orientación a responsables para el cumplimiento de los principios y deberes establecidos en la LGPDPPSO y la LPDPPSOEG.

Es importante precisar que la información utilizada para el cumplimiento de principios y deberes es **responsabilidad del usuario**, por lo que la utilización de la presente guía y su cumplimiento **dependerá de lo realizado por el responsable.**

La guía para el cumplimiento de principios y deberes **no equivale a una autorización ni a un visto bueno del ITAIGro**, si no que se limita a facilitar el cumplimiento de los multicitados ordenamientos de conformidad con los elementos que indica la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley número 466 de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Guerrero. Siendo esto último el objeto principal del documento orientador.