Protección de Datos Personales

INTRODUCCIÓN

El Centro de Investigación en Química Aplicada como dependencia de la Administración Pública, es sujeto obligado en términos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Por ello, es responsable de proteger los datos personales que trate, garantizando los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, los deberes de seguridad y confidencialidad, y las obligaciones derivadas de la Ley General.

El presente documento constituye una política interna, elaborado en observancia al principio de responsabilidad, el cual prevé que la o el responsable del tratamiento de los datos personales deberá implementar mecanismos para el cumplimiento de los principios, deberes y obligaciones establecidos en las disposiciones en materia de protección de datos personales.

Estos mecanismos, prevé la ley que deben tener por objeto establecer los elementos y las actividades de dirección, operación y control de todos sus procesos que, en el ejercicio de funciones y atribuciones, impliquen un tratamiento de datos personales a efecto de proteger éstos de manera sistemática y continua

La presente Política Interna de Protección de Datos Personales del CIQA fue aprobada por el Comité de Transparencia, al ser la autoridad máxima en materia de protección de datos personales de conformidad a los artículos 30, fracción 11, 83, 84, fracción 1 y 87 de la Ley General, y el artículo 47 de los Lineamientos Generales.

PROPÓSITO

Garantizar el cumplimiento de los principios, deberes y obligaciones en materia de protección de datos personales, establecer mejores prácticas y estándares, así como elementos y actividades de dirección, operación y control en los procesos en que las Unidades Administrativas, que en el ejercicio de sus atribuciones realicen algún tratamiento de datos personales.

ALCANCE

La presente Política de Protección de Datos Personales es de observancia general para todo el personal del CIQA involucrado en el tratamiento de datos personales.

La aplicación y cumplimiento de la presente Política de Protección de Datos Personales, es obligatoria para los Titulares de las Unidades Administrativas responsables de cualquier tratamiento de datos personales con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización, así como establecer las medidas necesarias que garanticen la seguridad de los datos personales que el ámbito de su competencia posean, recaben o transmitan, a fin de evitar su alteración, daño, destrucción o su uso, acceso o tratamiento no autorizado, pérdida y transmisión, debiendo asegurar su manejo para los propósitos para los cuales se hayan obtenido.

REFERENCIAS NORMATIVAS

- Constitución Política de los Estados Unidos Mexicanos, artículo 6°, Base Ay segundo párrafo del artículo 16.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Lineamientos que establecen los parámetros, modalidades y procesamiento para la portabilidad de datos personales.
- Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Lineamientos de actuación del Comité de Transparencia.

GLOSARIO

En adición a los términos establecidos en el artículo 3 de la Ley General, para efectos de los presentes lineamientos, se entenderá por:

Capacitación. - Medida de seguridad para establecer las políticas y procedimientos de entrenamiento basado en roles y responsabilidades.

Ciclo de vida. - Se refiere a las fases del tratamiento de los datos personales, consistentes en la obtención, almacenamiento, uso, divulgación, bloqueo y cancelación.

Comité de Transparencia. - Autoridad máxima en materia de datos personales.

Deberes. - Confidencialidad y de seguridad.

Enlace de datos personales. - Personas servidoras públicas designadas por las personas Titulares de las Unidades Administrativas, a efecto de fungir como enlace ante el Comité de Transparencia, en las responsabilidades que susciten en materia de protección de datos personales.

Inventario de datos personales. - Identificación de las bases de datos de tratamiento de las Unidades Administrativas, por el cual, se documenta la información básica de cada tratamiento realizado, con independencia de su forma de almacenamiento, entre lo cual se incluye el ciclo de vida del dato personal.

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

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

Órgano Garante. - Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Política. - Política de Protección de Datos Personales del CIQA

Portabilidad de Datos Personales. - Prerrogativa de los titulares de datos personales que les permite, bajo las condiciones establecidas en la normatividad aplicable, recibir los datos personales que han proporcionado a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable del tratamiento sin impedimentos.

Principios. - El derecho a la protección de los datos personales se regula a través de ocho principios, los cuales se traducen en obligaciones, estos son: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

Sujeto Obligado Receptor. - Cualquier autoridad, dependencia, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, tribunales administrativos, fideicomisos y fondos públicos y partidos políticos del orden federal, estatal o municipal, que recibe directamente los datos personales, en un formato estructurado y comúnmente utilizado, a petición del o la titular.

Titular. - La persona física a quien corresponden o conciernen los datos personales sujetos a tratamiento y por tanto es quien se considera como sujeto de protección del derecho a la protección de datos personales.

Titular de la Unidad Administrativa. - Persona responsable del tratamiento de los datos personales en la unidad administrativa a su cargo.

Disposiciones Generales

Artículo 1.- La presente Política de Protección de Datos Personales es de observancia general para todo el personal del CIQA involucrado en el tratamiento de datos personales.

El Comité de Transparencia como autoridad máxima en la materia velará por el debido cumplimiento y aplicación de la presente Política.

Artículo 2.- La Unidad de Transparencia asesorará a las Unidades Administrativas en materia de protección de datos personales conforme a los principios, deberes y obligaciones establecidos en la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

Artículo 3.- Para las actividades señaladas en la presente Política, será necesario contar con personas servidoras públicas que actúen como enlaces en materia de datos personales.

Artículo 4.- Las personas Titulares de las Unidades Administrativas son los responsables del tratamiento de los datos personales en el ámbito de sus facultades y atribuciones; y, por lo tanto, tendrán la obligación de cumplir los principios, deberes y obligaciones establecidos en la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

Artículo 5.- El Comité de Transparencia podrán sugerir a las Unidades Administrativas que realicen o dejen de hacer ciertas acciones con el fin de prevenir algún incumplimiento a las disposiciones en materia de protección de datos personales.

Artículo 6.- El Comité de Transparencia cuando advierta un hecho que pueda constituir una probable falta administrativa en materia de datos personales en términos de la normativa aplicable, darán vista al Órgano Interno de Control para su conocimiento.

Artículo 7.- El Comité de Transparencia, se auxiliará en la Dirección General para el ejercicio de sus funciones previstas en la presente Política.

De los Principios de Protección de Datos Personales

Los principios de protección de datos personales son las herramientas para garantizar la efectiva protección de los datos personales de sus titulares cuando son tratados; herramientas de uso obligatorio para interpretar y aplicar la Ley General y demás normativa aplicable y representar un límite al tratamiento de datos personales que se encuentran en posesión de sujetos obligados.

Artículo 8.- Las personas Titulares de las Unidades Administrativas, responsables del tratamiento de datos personales deberán observar los siguientes principios rectores de la protección de datos personales:

1) Licitud
2) Finalidad
3) Lealtad
4) Consentimiento
5) Calidad
6) Proporcionalidad
7) Información
8) Responsabilidad

Principio de Licitud

Artículo 9.- El tratamiento de datos personales por parte de las personas Titulares de las Unidades Administrativas debe ser realizado de conformidad con las atribuciones o facultades que previamente se otorgan en la normativa aplicable que le confiera, en este sentido, no deben tratarse datos personales si no se sujetan a las facultades previamente conferidas.

Obligación vinculada al Principio de Licitud

Artículo 10.- Es una obligación de las personas Titulares de las Unidades Administrativas, identificar el marco normativo que en el ámbito de sus atribuciones se encuentra relacionado con el tratamiento de datos personales, el tipo de datos objeto de tratamiento y las finalidades para ello, los cuales deben ser tratados de manera lícita.

Mecanismo para acreditar el cumplimiento del Principio de Licitud

Artículo 11.- Para acreditar el cumplimiento a este principio, las personas Titulares de las Unidades Administrativas, deberán incluir en el aviso integral y en el inventario de datos personales, el fundamento legal que les faculta tratar datos personales.

Principio de Finalidad

Artículo 12.- Todo tratamiento de datos personales efectuado por las personas Titulares de las Unidades Administrativas tendrá que estar justificado por las finalidades concretas, explícitas, lícitas y legítimas. Para tal efecto, se entenderá que las finalidades son:

Concretas: Atender el tratamiento de los datos personales con los fines específicos o determinados para los que fueron recabados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión a su titular;

Explícitas: Señalar y dar a conocer de manera clara en el aviso de privacidad las finalidades relativas al tratamiento de datos personales;

Lícitas: Las finalidades que justifiquen el tratamiento de los datos personales deben ser acordes con las atribuciones o facultades de la Unidad Administrativa conforme a la normatividad aplicable;

Legítimas: Cuando las finalidades que motivan el tratamiento de los datos personales se encuentran autorizadas por el consentimiento dé su titular, salvo que se actualicen las excepciones previstas en la Ley General, en la presente Política y demás normativa aplicable.

De este modo, la finalidad o finalidades del tratamiento de datos personales deberán ser determinadas, es decir, deberán especificar para qué objeto se tratarán los datos personales de manera clara, sin lugar a confusión y con objetividad.

Obligaciones vinculadas al Principio de Finalidad

Artículo 13.- Las obligaciones para su cumplimiento por parte de las personas Titulares de las Unidades Administrativas que traten datos personales, son las siguientes:

1) Tratar los datos personales únicamente para la finalidad o finalidades que hayan sido informadas a su titular en el aviso de privacidad y, en su caso, consentidas.
2) Informar en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales y redactarlas de forma tal que sean determinadas.
3) Identificar y distinguir en el aviso de privacidad entre las finalidades que dan origen al tratamiento de aquellas que son distintas a las que lo originaron, pero se consideran compatibles y/o análogas;
4) Ofrecer a la o el titular de los datos personales un mecanismo para que pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades secundarias;
5) Tratar los datos personales para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que se hubiese recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, al menos que lo permita una ley o reglamento, o se obtenga el consentimiento de la o el titular de los datos.

Mecanismos para acreditar el cumplimiento del Principio de Finalidad

Artículo 14.- Para acreditar el debido cumplimiento a este principio por parte de las personas Titulares de las Unidades Administrativas, se deberá realizar lo siguiente:

1) Contar con un inventario en el que se observen las finalidades de cada tratamiento que realice en su unidad administrativa, verificar que estas sean específicas y/o determinadas y que sean acordes a sus atribuciones o facultades.
2) Vigilar que las personas servidoras públicas a su cargo, únicamente traten datos personales en términos de las finalidades informadas en el aviso de privacidad correspondiente.
3) Verificar que en los avisos de privacidad informen, todas las finalidades para las cuales se tratan los datos personales y que éstas sean descritas de manera clara;
4) Informar a los y las titulares las finalidades sobre el tratamiento de sus datos personales;
5) Recabar el consentimiento de los y las titulares para el tratamiento de datos personales, cuando el mismo se requiera.

Principio de Lealtad

Artículo 15.- Las personas Titulares de las Unidades Administrativas se abstendrán de obtener y tratar datos personales a través de medios engañosos o fraudulentos. Con este principio no se permite un tratamiento tramposo, deshonesto y no ético de los datos personales de los y las titulares.

Obligaciones vinculadas al Principio de Lealtad

Artículo 16.- Las obligaciones para su cumplimiento por parte de las personas Titulares de las Unidades Administrativas que tratan datos personales, son las siguientes:

1) Verificar que los datos personales no se recaben con dolo, mala fe o negligencia;
2) Comprobar que el tratamiento de los datos personales no genere discriminación o un trato injusto o arbitrario contra sus titulares;
3) Evitar quebrantar la confianza de los y las titulares en relación con sus datos
4) personales que serán tratados conforme a lo acordado;
5) Informar todas las finalidades del tratamiento en el aviso de privacidad.

Mecanismos para acreditar el cumplimiento del Principio de Lealtad

Artículo 17.- Para acreditar el cumplimiento a este principio por parte de las personas Titulares de las Unidades Administrativas, se deberá realizar lo siguiente:

1) Contar con avisos de privacidad que cumplan con lo establecido en la Ley General, la presente Política y demás normativa aplicable;
2) Implementar instrumentos que permitan verificar que los tratamientos realizados no den lugar a discriminación, trato injusto o arbitrario en contra de la o el titular;
3) Constatar que el tratamiento de datos personales sólo se lleve a cabo para los fines informados en el aviso de privacidad.

Principio de Consentimiento

Artículo 18.- Previo al tratamiento de los datos personales, las personas Titulares de las Unidades Administrativas deberán obtener el consentimiento de las y los titulares de los datos personales de manera libre, específica, inequívoca e informada, salvo que no sea requerido, en virtud de las siguientes causales de excepción:

1) Cuando una ley así lo disponga, en cuyo caso, los supuestos de excepción deberán ser acordes con las bases, principios y disposiciones establecidos en la Ley General que, en ningún caso, podrán contravenirla;
2) Cuando las transferencias que se realicen con otro sujeto responsable sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles y acordes con la finalidad que motivó el tratamiento de los datos personales;
3) Cuando exista una orden judicial, resolución o mandato fundado y motivado de
4) autoridad competente;
5) Para el reconocimiento o defensa de derechos de la titular ante autoridad competente;
6) Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el o la titular y el CIQA.
7) Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
8) Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico o la prestación de asistencia sanitaria;
9) Cuando los datos personales figuren en fuentes de acceso público;
10) Cuando los datos personales se sometan a un procedimiento previo de disociación.
11) Cuando la o el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

La actualización de alguno de los supuestos no exime a las personas Titulares de las Unidades Administrativas responsables del tratamiento de datos personales del cumplimiento de las demás obligaciones establecidas en la Ley General, en la presente Política y demás normativa aplicable.

Este principio de consentimiento obliga a las personas Titulares de las Unidades Administrativas, en caso de no estar dentro alguna de las excepciones previstas anteriormente, a solicitar el consentimiento del titular para el tratamiento de sus datos personales.

Por regla general, el consentimiento tácito será válido para llevar a cabo el tratamiento de datos personales, salvo aquellos supuestos en los cuales la Ley General o alguna disposición aplicable exija su obtención de forma expresa y, en su caso, por escrito, particularmente, cuando se refiera a datos sensibles.

Obligaciones vinculadas al Principio de Consentimiento

Artículo 19.- Las obligaciones para su cumplimiento por parte de las personas Titulares de las Unidades Administrativas que traten datos personales, son las siguientes:

1) Obtener el consentimiento de la o el titular, previo al tratamiento de los datos personales, salvo que se actualice alguno de los supuestos de excepción descritos anteriormente;
2) Recabar el consentimiento expreso y, en su caso, por escrito, a través de formatos claros y sencillos, acorde con el perfil de la o el titular, en los cuales se distingan los datos personales y finalidades del tratamiento que requieren de la manifestación de su voluntad;
3) Implementar medios sencillos y gratuitos para la obtención del consentimiento, independientemente de la modalidad en que se requiera;
4) En su caso, habilitar en el aviso de privacidad casillas y/o espacios para que la o el titular exprese su consentimiento, respecto de cada una de las finalidades para las cuales son tratados sus datos personales.

Mecanismos para acreditar el cumplimiento del Principio de Consentimiento

Artículo 20.- Para acreditar el cumplimiento a este principio por parte de las personas Titulares de las Unidades Administrativas, se deberá realizar lo siguiente:

1) Identificar en el aviso de privacidad, aquellos datos personales y finalidades que requieren del consentimiento de su titular, para su tratamiento;

2) Mantener bajo su resguardo una copia del documento en el cual se haya manifestado el consentimiento de la o el titular para el tratamiento de sus datos, cuando éste proceda;
3) Documentar la puesta a disposición del aviso de privacidad a la o el titular, en aquellos casos en los cuales sea válidos el consentimiento tácito.

Principio de Información

Artículo 21.- Las personas Titulares de las Unidades Administrativas que traten datos personales, se encuentran obligadas a informar a las personas titulares, las características principales del tratamiento al que será sometida su información personal, lo que se materializa a través del aviso de privacidad. En ese sentido, se deberá elaborar y poner a disposición los avisos de privacidad simplificado e integral que correspondan al tratamiento que lleven a cabo, en los términos establecidos en la Ley General, en la presente Política y demás normativa aplicable, independientemente de que se requiera o no el consentimiento del o la titular.

Obligaciones vinculadas al Principio de Información

Artículo 22.- Las obligaciones para su cumplimiento por parte de las personas Titulares de las Unidades Administrativas que traten datos personales, son las siguientes:

1) Redactar el aviso de privacidad en sus dos modalidades: integral y simplificado, con las características principales del tratamiento al que serán sometidos los datos personales de su titular, estructurado de manera clara y sencilla que facilite su entendimiento y con los elementos establecidos por la Ley General y los Lineamientos Generales;
2) Poner a disposición de las y los titulares el aviso de privacidad en los términos que fije la Ley General y los Lineamientos Generales, aunque no se requiera el consentimiento para el tratamiento de sus datos personales;
3) Remitir los avisos de privacidad en ambas modalidades al Comité de Transparencia para su revisión, para que en su caso, emita los comentarios respectivos o el visto bueno de los mismos;
4) Difundir, poner a disposición o reproducir el aviso de privacidad en formatos físicos y electrónicos, ópticos, sonoros, visuales o a través de cualquier otra tecnología que permita su eficaz comunicación y permitan la accesibilidad para grupos vulnerables;
5) Solicitar a la Dirección General, la publicación en el portal de Internet el aviso de privacidad integral;

6) Incorporar el aviso de privacidad simplificado en un lugar visible y específico que facilite la consulta de los y las titulares, independientemente del tipo de soporte ya sea físico o electrónico en el que se encuentre el tratamiento de los datos personales.
7) Comunicar en el aviso de privacidad simplificado e integral, la información relativa en caso de haber transferencias;
8) Prever excepcionalmente o cuando resulte imposible dar a conocer a las y los titulares el aviso de privacidad de manera directa o ello exija esfuerzos desproporcionados, instrumentar algún mecanismo o medidas para la comunicación masiva del aviso de privacidad.

Estos mecanismos o medidas, en términos de la Ley General, se conocen como medidas compensatorias: son mecanismos alternos para dar a conocer el aviso de privacidad a través de medios de amplio alcance, utilizado de manera inusual por los responsables del tratamiento de datos personales.

En el caso anterior, la persona Titular de la Unidad Administrativa deberá solicitar la asesoría correspondiente.

Mecanismos para acreditar el cumplimiento del Principio de Información

Artículo 23.- Para acreditar el cumplimiento de este principio por parte de las personas Titulares de las Unidades Administrativas, se deberá realizar lo siguiente:

1) Contar con los avisos de privacidad integral y simplificado por cada proceso de tratamiento de datos personales que se lleve a cabo;
2) Implementar un procedimiento o medio para la puesta de disposición del aviso de privacidad;
3) Realizar las gestiones para que los avisos de privacidad, en sus modalidades simplificado e integral, sean plasmados en un lugar visible que permita la consulta del o la titular, conforme a lo establecido en las obligaciones señaladas en el artículo anterior;
4) Incluir en el inventario los lugares y medios en los que se difunden y colocan los avisos de privacidad;
5) Documentar la comunicación realizada del aviso de privacidad a terceras personas a las que se transfieran los datos personales.

Principio de Proporcionalidad

Artículo 24.- Las personas Titulares de las Unidades Administrativas, recabarán aquellos datos personales que resulten necesarios, adecuados y relevantes para la finalidad que justifica su tratamiento. Se entenderá que los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención, de acuerdo con las atribuciones conferidas.

Obligaciones vinculadas al Principio de Proporcionalidad

Artículo 25.- Las obligaciones para su cumplimiento por parte de las Unidades Administrativas que traten datos personales, son las siguientes:

1) Recabar y tratar sólo aquellos datos personales necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron. y, en su caso, privilegiar la utilización de datos generados, para que el tratamiento de datos personales de la o el titular no sea excesivo, como por ejemplo usar el número de empleado en lugar de la CURP o el RFC;
2) Realizar esfuerzos razonables para limitar los datos personales tratados al mínimo necesario, considerando las finalidades que motivan su tratamiento;
3) Limitar al mínimo posible el periodo de tratamiento de datos personales;
4) Verificar si los datos personales que serán requeridos por la persona Titular de la Unidad Administrativa para su tratamiento ya son tratados por otra persona Titular de una Unidad Administrativa diversa a la anterior.

Mecanismos para acreditar el cumplimiento del Principio de Proporcionalidad.

Artículo 26.- Para acreditar el debido cumplimiento a este principio por parte de las personas Titulares de las Unidades Administrativas, deberá realizar lo siguiente:

1) Analizar y revisar que en su área se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate;
2) Establecer con precisión los datos personales que deberán tratarse para cumplir con la finalidad, cuando una normativa establezca su obtención, sólo se deberán solicitar dichos datos;
3) Promover prácticas que minimicen la obtención de datos personales.

Principio de Calidad

Artículo 27.- Las personas Titulares de las Unidades Administrativas, deberán mantener los datos personales conforme a la finalidad o finalidades para las que se hayan recabado y adoptar las medidas necesarias para mantenerlos exactos, correctos, completos y actualizados.

1) 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;
2) Correctos: son correctos cuando no presentan errores que pudieran afectar su veracidad;
3) Completos: cuando la integridad de los datos personales permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del o la responsable;
4) Actualizados: cuando los datos personales responden fielmente a la situación actual de su titular.

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

Las personas Titulares de las Unidades Administrativas responsables deberán adoptar las medidas para garantizar que los datos personales cumplan con las características del Principio de Calidad, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que la o el titular se vea afectado por dicha situación.

En el supuesto de que los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones aplicables, serán suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación.

Obligaciones vinculadas al Principio de Calidad

Artículo 28.- Las obligaciones para su cumplimiento por parte de las personas Titulares de las Unidades Administrativas que traten datos personales, son las siguientes:

1) Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales, principalmente cuando se obtuvieron de manera indirecta de la o el titular;
2) Establecer plazos de conservación de la información, conforme a las disposiciones legales aplicables en materia archivística;

3) Establecer y documentar los procedimientos para la conservación, bloqueo y supresión de los datos personales.

Mecanismos para acreditar el cumplimiento del Principio de Calidad

Artículo 29.- Para acreditar el debido cumplimiento de este principio por parte de las Unidades Administrativas, se deberá realizar lo siguiente:

1) Generar una relación de todas las bases de datos con que cuentan y el tipo de información personal tratada en cada una de ellas que, en su caso, permita vincularlas;
2) Documentar las actualizaciones y supresiones realizadas;
3) Contar con los procedimientos para la conservación, bloqueo y supresión de los datos personales.

Principio de Responsabilidad

Artículo 30.- Conforme al principio de responsabilidad, las personas Titulares de las Unidades Administrativas velarán por el cumplimiento del resto de los principios, adoptar medidas necesarias como estándares y mejores prácticas para su aplicación y demostrar ante las y los titulares y al Órgano garante que cumple con sus obligaciones en torno a la protección de datos personales.

Asimismo, el Principio de Responsabilidad también es conocido por el principio de rendición de cuentas, ya que como bien se dijo en el párrafo anterior, establece la obligación de velar por el cumplimiento del resto de los principios, así como los deberes que establece la normativa aplicable para dar cuenta a los y las titulares y la autoridad de que se cumple con las obligaciones de protección de datos personales. Por ello, la Unidad de Transparencia será la encargada de pedir cuentas a las Unidades Administrativas en materia de protección de datos personales.

Obligaciones vinculadas al Principio de Responsabilidad

Artículo 31.- Las obligaciones para su cumplimiento por parte de las personas Titulares de las Unidades Administrativas que traten datos personales, son las siguientes:

1) Participar en los programas de capacitación y actualización en materia de protección de datos personales;
2) Establecer procedimientos para recibir y responder dudas y quejas de los y las titulares;

3) Diseñar o modificar las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología con que cuente y que implique el tratamiento de datos personales, para que desde el inicio cumplan por diseño con las obligaciones previstas en la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable;
4) Cumplir con los principios y deberes que establece la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

Artículo 32.- Las obligaciones para el cumplimiento del Principio de Responsabilidad:

1) Recopilar de las Unidades Administrativas que traten datos personales, los insumos necesarios para elaborar un Programa de Protección de Datos Personales que provea los elementos y actividades de dirección, operación y control de los procesos, para proteger de manera sistemática y continua de los datos personales;
2) Diseñar e implementar programas de capacitación y actualización que tengan por obligación capacitar al personal involucrado en el tratamiento de datos personales;
3) Recopilar de las Unidades Administrativas que traten datos personales, los insumos necesarios para la elaboración del Documento de Seguridad que contemple las medidas de carácter administrativo, técnico, físico o cualquier otra;
4) Revisar periódicamente el Programa de Protección de Datos Personales y el Documento de Seguridad para determinar las modificaciones que se requieran;
5) Revisar el cumplimiento de los procedimientos para recibir y responder dudas y quejas de las y los titulares;
6) Realizar y vigilar el procedimiento para el tratamiento de datos personales en políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología de diseño o modificación para que cumplan con las obligaciones previstas en la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable;
7) Implementar mecanismos y/o realizar acciones para asegurar y acreditar el cumplimiento de los principios y deberes que establece la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

Mecanismos para acreditar el cumplimiento del Principio de Responsabilidad

Artículo 33.-Para acreditar el debido cumplimiento al Principio de Responsabilidad por parte de las Unidades Administrativas, se deberá realizar lo siguiente:

1) Contar con las constancias de capacitación en materia de protección de datos personales;
2) Llevar un registro de las dudas y quejas de los y las titulares de datos personales;
3) Documentar la comunicación relacionada con el diseño o modificación de las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología con que cuente y que implique el tratamiento de datos personales;
4) Documentar la comunicación relacionada con el cumplimiento de los principios y deberes que establece la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

Artículo 34.- Para acreditar el debido cumplimiento del Principio de Responsabilidad:

1) Coordinar el Programa en materia de Protección de Datos Personales y el Documento de Seguridad;
2) Acreditar la capacitación con las listas de asistencia a los cursos en materia de protección de datos personales;
3) Realizar en su caso, la actualización del Programa de Protección de Datos Personales y el Documento de Seguridad;
4) Evidenciar del cumplimiento de los procedimientos para recibir y responder dudas y quejas de las y los titulares;
5) Documentar y observar el cumplimiento del procedimiento para el tratamiento de datos personales en políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología de diseño o modificación que cumplan con las obligaciones previstas en la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable;
6) Guardar evidencia de los mecanismos y/o acciones para asegurar y acreditar el cumplimiento de los principios y deberes que establece la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

De la implementación o modificación de bases de datos

Artículo 35.- En relación con el debido cumplimiento del principio de responsabilidad, se implementará un procedimiento para garantizar la gobernabilidad en la protección de los datos personales.

Propósito del procedimiento

Artículo 36.- El procedimiento tendrá el propósito de asesorar a las personas Titulares de las Unidades Administrativas que pretendan dar tratamiento de datos personales que obren en soportes físicos como electrónicos, en términos del artículo 85, fracción VII de la Ley General.

Artículo 37.- Las personas Titulares de las Unidades Administrativas previo a recabar datos personales deberán solicitar la opinión o asesoría, Conforme a lo anterior, las personas Titulares de las Unidades de las Unidades Administrativas tendrán que adjuntar a su solicitud una ficha técnica debidamente requisitada, donde se indique lo siguiente:

1) El objetivo de la implementación o modificación de la base de datos;
2) Fundamento legal conforme a sus facultades o atribuciones de la normativa;
3) Justificación de la necesidad de implementar o modificar la base datos personales;
4) Los datos personales que serán objeto de tratamiento;
5) Los datos personales sensibles que serán objetos de tratamiento;
6) Las finalidades del tratamiento;
7) Los procesos, las fases o actividades operativas de las bases de datos que involucren tratamiento de datos personales;
8) La obtención de los datos personales;
9) Señalar si se pretende efectuar transferencias de datos personales y sus finalidades;
10) Señalar si se pretende efectuarse remisiones de datos personales y sus finalidades;
11) El tiempo de duración de la base de datos personales;
12) Plazo de conservación o almacenamiento de los datos personales;
13) La tecnología que se pretende utilizar para efectuar el tratamiento de los datos personales;
14) Las medidas de seguridad físicas, administrativas y técnicas;
15) Cualquier otra información o documentos que se considere conveniente de hacer del conocimiento respecto a la base de datos que se pretende implementar o modificar.

Artículo 38.- El Comité de Transparencia deberá emitir el dictamen de tratamiento de datos personales, en el que se exponga si la implementación o modificación de la base datos personales cumple con los principios, deberes y obligaciones de la Ley General, los Lineamientos Generales y normativa aplicable en materia de protección de datos personales en un plazo no mayor de veinte días hábiles.

De los Deberes para la Protección de Datos Personales

La protección de los datos personales además de los principios y las obligaciones ya expuestas prevé dos deberes, el de confidencialidad y el de seguridad.

La importancia de estos deberes es proteger los datos personales de cualquier amenaza de riesgo con potencial para provocarles un daño o perjuicio, como el robo, extravío o copia no autorizada, pérdida o destrucción no autorizada, uso o acceso no autorizado, daño, alteración o modificación no autorizado.

Artículo 39.- Además de los principios señalados en el Capítulo anterior, las personas Titulares de las Unidades Administrativas deberán cumplir con los siguientes deberes:

1) Deber de Confidencialidad
2) Deber de Seguridad

Deber de Confidencialidad

Artículo 40.- Las personas Titulares de las Unidades Administrativas que traten datos personales deberán establecer controles o mecanismos de observancia obligatoria para las personas servidoras públicas que intervengan en cualquier fase del tratamiento, mantengan en secreto la información, así como evitar que los datos personales sean revelados a personas no autorizadas y prevenir la divulgación no autorizada de los mismos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

Es así como, dicho deber implica la obligación de guardar secreto respecto de los datos personales que son tratados por las personas Titulares de las Unidades Administrativas, para evitar causar un daño a su titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información y hacer mal uso de esta.

Obligaciones vinculadas al Deber de Confidencialidad

Artículo 41.-Las obligaciones para su cumplimiento por parte de las personas Titulares de las Unidades Administrativas que traten datos personales son:

1) Prever controles mediante los cuales se garantice la confidencialidad de los datos personales que son tratados;
2) Establecer cláusulas en los contratos para que los sujetos obligados del ámbito público o privado a los cuales les sean transferidos o remitidos datos personales se obliguen a la confidencialidad de éstos durante y posterior a la vigencia del instrumento jurídico ;
3) Implementar campañas de sensibilización para las personas servidoras públicas, sobre la importancia de la confidencialidad de los datos personales;
4) Proponer la implementación de mejores prácticas al interior para garantizar la secrecía de los datos personales.

Mecanismos para acreditar el Deber de Confidencialidad

Artículo 42.- Para acreditar el cumplimiento a este deber por parte de las personas Titulares de las Unidades Administrativas, se deberá realizar lo siguiente:

1) Incluir en el Documento de Seguridad, los controles y las medidas de seguridad implementadas para garantizar la secrecía de los datos personales;
2) Generar evidencia de los controles implementados para garantizar la confidencialidad de los datos;
3) Contar con los contratos en los cuales se establezcan las cláusulas de confidencialidad de datos, respecto de transferencias o remisiones;
4) Tener la evidencia documental de los cursos, talleres, seminarios o similares en los que haya participado el personal de las Unidades Administrativas y se encuentren relacionados con la materia de protección de datos personales;
5) Documentar la implementación de mejores prácticas que garanticen la confidencialidad de los datos tratados .

Deber de Seguridad

Artículo 43.- Las personas Titulares de las Unidades Administrativas, adoptarán e instrumentarán las medidas físicas, técnicas y administrativas a través de las cuales garantice la protección de datos personales.

Obligaciones vinculadas al Deber de Seguridad

Artículo 44.- Las obligaciones para su cumplimiento por parte de las personas Titulares de las Unidades Administrativas que traten datos personales son:

1) Generar e implementar políticas de gestión, en las cuales se considere el tipo de datos personales recabados, el tratamiento que se les dará y el ciclo de vida, es decir, su obtención, uso y posterior supresión;
2) Establecer las personas servidoras públicas que podrán intervenir en el tratamiento de los datos personales y definir las funciones y obligaciones que tendrán;
3) Realizar un análisis de riesgo de los datos personales tratados, así como de los sistemas físicos y/o electrónicos en los cuales se desarrolle dicho tratamiento; ·
4) Desarrollar acciones de prevención y mitigación de amenazas o vulneraciones de datos personales;
5) Monitorear y revisar las medidas de seguridad adoptadas para garantizar la protección de datos;

6) Incentivar la capacitación de las personas servidoras públicas involucradas en el tratamiento de datos personales, conforme al nivel de responsabilidad que tengan asignado.

Mecanismos para acreditar el Deber de Seguridad

Artículo 45.- Para acreditar el cumplimiento de este deber por parte de las personas Titulares de las Unidades Administrativas, se deberá realizar lo siguiente :

1) Contar con un inventario de las bases de datos personales;
2) Describir los roles y las responsabilidades específicas de las personas servidoras públicas relacionadas con el tratamiento de datos personales;
3) Implementar mecanismos y/o políticas para la protección de datos y guardar evidencia de ello;
4) Llevar una bitácora en la cual se asiente cualquier amenaza o vulneración de datos personales suscitada, así como de las acciones realizadas para su mitigación;
5) Instrumentar las medidas de seguridad físicas, técnicas y administrativas adoptadas para garantizar el tratamiento de los datos recabados, así como las acciones de monitoreo, análisis y revisión a implementar, a fin de mantenerlas actualizadas y, en su caso, detectar áreas de oportunidad para su desarrollo y ejecución;
6) Tener la evidencia documental de los cursos, talleres, seminarios o similares en los que haya participado el personal de la Unidad Administrativa y se encuentren relacionados con la materia de protección de datos personales.

Documentos para la Protección de Datos Personales

Para la Protección de Datos Personales, se contará con los siguientes documentos:

Documento de Seguridad. Documento elaborado en coordinación con las Unidades Administrativas , cuyo propósito es establecer las medidas administrativas, físicas y técnicas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Programa de Protección de Datos Personales. Documento de planeación que tiene por objeto establecer elementos y actividades de dirección, operación y control de los procesos de la organización, para proteger de manera sistemática y continúa los datos personales.

Programa de Capacitación. Documento en el cual se prevén actividades de capacitación y actualización para todo el personal de la Secretaría, considerando sus roles y responsabilidades asignadas para el tratamiento de datos personales.

Aviso de Privacidad. Documento generado por las Unidades Administrativas, para dar a conocer a las y los titulares los datos personales que son recabados y las finalidades de su tratamiento .

Documento de Seguridad

Artículo 46.- La Secretaría deberá contar con un Documento de Seguridad como parte de los mecanismos implementados para asegurar el cumplimiento del deber de seguridad, cuyo objeto es describir y dar cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas, para la protección de datos personales que permitan protegerlos contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

El Documento de Seguridad deberá de ser aprobado por el Comité de Transparencia .

Artículo 47.- El Documento de Seguridad deberá contener como mínimo, lo siguiente:

1) El inventario de datos personales y de los sistemas de tratamiento;
2) Las funciones y obligaciones de las personas que traten datos personales;
3) El análisis de riesgos;
4) El análisis de brecha;
5) El plan de trabajo;
6) Los mecanismos de monitoreo y revisión de las medidas de seguridad;
7) El programa general de capacitación.

Vigencia y Actualización

Artículo 48.- En las actualizaciones que se realicen al Documento de Seguridad deberán participar las personas Titulares de las Unidades Administrativas, a través de sus enlaces en materia de datos personales, quienes en todo momento observarán los principios, deberes y obligaciones a los que se refieren la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

Para la formulación de propuestas de actualización del Documento de Seguridad, se elaborarán formatos, cuestionarios o cualquier otro instrumento de apoyo, que resulten útiles para el cumplimiento de esta Política y demás disposiciones aplicables en la materia.

Acorde con lo dispuesto en la Ley General, el Documento de Seguridad se actualizará en los supuestos siguientes:

1) Se produzcan modificaciones sustanciales al tratamiento de los datos personales que deriven en un cambio de nivel de riesgo;
2) Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión con el que se cuente;
3) Derivado de un proceso de mejora para mitigar el impacto de vulneración a la seguridad ocurrida;
4) Con motivo de la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Con independencia de los supuestos anteriores, el Documento de Seguridad podrá ser actualizado cada dos años.

Artículo 49.- Cuando alguna de las personas Titulares de las Unidades Administrativas se encuentre en algunos de los supuestos del artículo anterior, la o el enlace solicitará por escrito las actualizaciones conducentes y se resolverá lo conveniente y lo someterá al Comité de Transparencia .

Las personas enlaces podrán solicitar la orientación necesaria, para la integración o cualquier acto relacionado con los alcances del Documento de Seguridad.

Vulneraciones a la Seguridad de los Datos Personales

Artículo 50.- En términos de lo previsto en la Ley General, se consideran como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

1) La pérdida o destrucción no autorizada;
2) El robo, extravío o copia no autorizada;
3) El uso, acceso o tratamiento no autorizado;
4) El daño, la alteración o modificación no autorizada.

Artículo 51.- Las personas Titulares de las Unidades Administrativas deberán llevar una bitácora de las vulneraciones a la seguridad en las que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

Artículo 52.- Cuando las vulneraciones afecten de forma significativa los derechos patrimoniales o morales de las titulares de los datos personales, las personas Titulares de las Unidades Administrativas involucradas, deberán generar un informe detallado que contenga al menos lo siguiente:

1) La hora y fecha de la identificación de la vulneración;
2) La hora y fecha del inicio de la investigación sobre la vulneración;
3) La naturaleza del incidente o vulneración ocurrida;
4) La descripción detallada de las circunstancias en torno a la vulneración ocurrida;
5) Las categorías y número aproximado de personas titulares afectadas;
6) Los sistemas de tratamiento y datos personales comprometidos;
7) Las acciones correctivas realizadas de forma inmediata;
8) La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;
9) Las recomendaciones dirigidas a las y los titulares;
10) El medio puesto a disposición del o la titular para que pueda obtener mayor información sobre la vulneración y cómo proteger sus datos personales;
11) El nombre completo de la o las personas designadas para proporcionar mayor información al Órgano garante, en caso de requerirse;
12) Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Órgano garante.

Para efectos del presente artículo, se entenderá que se afectan los derechos patrimoniales de la o el titular, cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus bienes, información fiscal, historial crediticio, ingresos o egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados u otros similares.

De la misma manera, se entenderá que se afectan los derechos morales del o la titular, cuando la vulneración esté relacionada de manera enunciativa más no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, aspecto físico o menoscabe ilegalmente la libertad, integridad física o psíquica de la titular de los datos.

Artículo 53.- Las personas Titulares de las Unidades Administrativas tendrán la obligación de notificar a la(s} persona(s) titular(es) afectada(s). la información descrita en lo incisos anteriores, a través del medio que se establezca para ese fin.

En aquellos casos en los cuales no sea posible notificar directamente a la(s) personas (s) titular(es) afectada(s) sobre el informe a que hace referencia la presente Política o ello implique esfuerzos desproporcionados, se instrumentarán medidas compensatorias de comunicación para tal efecto, como son: la publicación en el periódico oficial, aviso en la

página oficial de Internet, sitios de internet, plataformas, tarjetas o cápsulas informativas u otro similar.

Artículo 54.- El informe al que se refiere el artículo 52 de la presente Política, las personas Titulares de las Unidades Administrativas deberán remitir a la en un plazo no mayor de cuarenta y ocho horas posteriores a que se haya confirmado la vulneración de seguridad, para que ésta la haga del conocimiento al Órgano garante en tiempo y forma, de conformidad con la Ley General, los Lineamientos Generales y demás normativa aplicable.

Artículo 55.- En términos de lo previsto en el artículo anterior, se deberá informar al Comité de Transparencia de lo ocurrido en torno a la vulneración de seguridad de datos personales.

Artículo 56.- El Comité de Transparencia podrá determinar la implementación de acciones adicionales a las realizadas por las personas Titulares de las Unidades Administrativas para evitar futuras vulneraciones y reforzar las medidas de seguridad existentes.

Para tal efecto, el Comité de Transparencia podrá auxiliarse de la asesoría, orientación o apoyo de las personas Titulares de las Unidades Administrativas, en asuntos de su especialidad, con la finalidad de garantizar la efectiva protección de los datos personales.

Para llevar a cabo lo anterior, el Comité de Transparencia se apoyará de la Dirección General para llevar a cabo dichas gestiones ante las personas Titulares de las Unidades de Administrativas.

Programa de Protección de Datos Personales

Artículo 57.- El CIQA deberá contar con un Programa de Protección de Datos Personales aprobado por el Comité de Transparencia, cuyo objetivo serán los siguientes:

1) Proveer el marco de trabajo necesario para la protección de los datos personales en posesión del CIQA;
2) Cumplir con los principios, deberes y obligaciones de la Ley General, la presente Política y la normatividad que derive de los mismos;
3) Establecer los elementos y las actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua;
4) Promover la adopción de mejores prácticas en la protección de datos personales, de manera preferente una vez que el programa se haya implementado de manera integral, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos específicos.

Artículo 58.- El Programa de Protección de Datos Personales deberá estar actualizado a fin de garantizar el desarrollo Ininterrumpido de actividades, sin demerito de que podrá ser sometido a su revisión o reajuste por parte del Comité de Transparencia, de conformidad con las facultades y atribuciones que le establece la normativa aplicable, en caso de estimarse necesario.

Artículo 59.- El Comité de Transparencia tendrá las siguientes funciones en relación al Programa de Protección de Datos Personales:

1) Elaborar y coordinar el Programa en conjunto con las Unidades Administrativas que estime necesario involucrar o consultar;
2) Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;
3) Dar a conocer el Programa al interior del sujeto obligado;
4) Coordinar la implementación del Programa en las Unidades Administrativas;
5) Asesorar a las Unidades Administrativas en la implementación del Programa, con el apoyo de las áreas técnicas que estime pertinente;
6) Revisar la correcta implementación del Programa;
7) Las demás que de manera expresa señale el propio Programa.

Artículo 60. El Programa de Protección de Datos Personales, deberá contener al menos:

1) Un diagnóstico sobre los problemas, las necesidades o áreas de oportunidad detectadas para el debido cumplimiento de los principios y deberes en materia de protección de datos personales;
2) Las actividades propuestas, su viabilidad, así como los objetivos que se persiguen, los cuales estarán vinculados a la atención de los problemas, las necesidades o áreas de oportunidad previamente detectadas;
3) Los mecanismos de revisión de los cuales se velará su cumplimiento.

Aviso de Privacidad

Artículo 61.- Como parte de las acciones para cumplir con el principio de información, se contará con un aviso de privacidad integral y su correlativo aviso de privacidad simplificado, por cada tratamiento de datos personales.

Excepcionalmente, cuando dos o más tratamientos de datos personales, atiendan una misma finalidad o función, se podrá contar con un mismo aviso de privacidad, en sus dos modalidades, siempre y cuando sea posible expresar con precisión y claridad las finalidades

del tratamiento de datos personales, de tal suerte que no dé lugar a incertidumbre o ambigüedad a sus titulares.

Elaboración o actualización

Artículo 62.- Los formatos para la elaboración de los avisos de privacidad integral y simplificado serán acordes con los elementos que establecen en la Ley General, los Lineamientos Generales y demás normatividad que resulte aplicable

Artículo 63. En la integración y elaboración de los avisos de privacidad, las Unidades Administrativas preverán un diseño que facilite su entendimiento por parte de las y los titulares de los datos.

En todo momento, los Titulares de las Unidades Administrativas, deberán asegurarse de que los avisos de privacidad se encuentren actualizados.

Redacción

Artículo 64. Las personas Titulares de las Unidades Administrativas se asegurarán de que la información asentada en los avisos de privacidad se encuentre redactada en un lenguaje ciudadano, sencillo, claro y comprensible, considerando en todo momento el perfil de la o el titular al cual vaya dirigido, por lo que se abstendrán de:

1) Usar frases inexactas, ambiguas o vagas;
2) Incluir textos que induzcan a los y las titulares a elegir una opción en específico;
3) Marcar previamente casillas, en caso de que éstas se incluyan, para que los y las titulares otorguen su consentimiento, o bien, incluir declaraciones orientadas a afirmar que los y las titulares ha consentido el tratamiento de sus datos personales sin manifestación alguna de su parte;
4) Remitir a textos o documentos que no estén disponibles para las y los titulares.

Artículo 65. Para la elaboración o actualización de los avisos de privacidad, las personas enlaces responsables podrán en todo momento, solicitar asesoría.

Casos en los que se requiere un nuevo Aviso de Privacidad

Artículo 66. En sustitución de los avisos de privacidad ya existentes, las personas Titulares de las Unidades Administrativas, considerarán la elaboración de un nuevo aviso de privacidad, en sus dos modalidades, cuando:

1) Por disposición del Reglamento Interior;
2) Requiera recabar datos personales sensibles adicionales a aquéllos informados aviso de privacidad original, los cuales no se obtengan de manera directa de la titular y se requiera de su consentimiento para el tratamiento de éstos;
3) Cambie las finalidades señaladas en el aviso de privacidad original;
4) Modifique las condiciones de las transferencias de datos personales o se pretendan realizar otras no previstas inicialmente y sean necesario el consentimiento del o la titular.

Programa de Capacitación y Actualización

Artículo 67. El CIQA contará con un Programa de Capacitación y Actualización en materia de Protección de Datos Personales, como uno de los mecanismos a través de los cuales se cumple con el principio de responsabilidad, el cual considerará los niveles de capacitación atendiendo los roles y las responsabilidades de las personas servidoras públicas que tratan la información personal, de conformidad con el artículo 24, fracción XIV del Reglamento Interior.

Elaboración y Aprobación

Artículo 68. El Comité de Transparencia será el órgano encargado de aprobar el Programa de Capacitación y Actualización en la materia, con base en la propuesta que sea presentada, en la cual se consideren las necesidades de capacitación de las Unidades Administrativas.

Operación

Artículo 69. El Comité de transparencia coordinará y dará seguimiento a los programas de capacitación continua y especializada en la materia de protección de datos personales.

Ejercicio de los Derechos ARCO y la Portabilidad de los Datos Personales

Artículo 70. Para efectos de la presente Política, se considera que los derechos ARCO comprenden el acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Artículo 71.- Cuando los datos personales se encuentren en un formato estructurado y comúnmente utilizado podrá proceder la portabilidad de los datos personales. Para realizar la portabilidad de datos personales.

De las Remisiones y Transferencias de los Datos Personales

Artículo 72.- La figura de la o el encargado, es una persona prestadora de servicios que trata datos personales a nombre de la persona Titular de la Unidad Administrativa responsable de los datos personales.

Esta figura tiene las siguientes características: puede ser una persona física o jurídica, de ámbito público o privado, puede ser una sola persona o de manera conjunta con otras personas, no tiene poder de decisión sobre el alcance y contenido del tratamiento de los datos personales y debe delimitar sus actuaciones a lo que diga la persona Titular de la Unidad Administrativa responsable de los datos personales.22

En relación con lo anterior, toda comunicación de datos personales realizada por la persona Titular de la Unidad Administrativa y la o el encargado dentro y fuera del territorio mexicano, se le conoce como remisión.

Artículo 73.- Las personas Titulares de las Unidades Administrativas que requieran encargar el tratamiento de datos personales, deberán pedir la opinión o asesoría del Comité de Transparencia.

Artículo 74.- La transferencia es toda comunicación de datos personales, dentro o fuera del territorio nacional, a persona distinta de la o el titular, de la persona Titular de la Unidad Administrativa o la o el encargado.

Artículo 75.- Las personas Titulares de las Unidades Administrativas que requieran realizar transferencias a terceras personas, de datos personales en su posesión deberán pedir la opinión o asesoría del Comité de Transparencia.

Artículo 76.- Toda transferencia de datos personales se encuentra sujeta al consentimiento de su titular. Para tal efecto, a través del aviso de privacidad correspondiente informarán al o la titular de los datos personales, las finalidades de la transferencia, así como el tercero receptor.

Supervisión en materia de Protección de Datos Personales

Artículo 77.- Para el debido cumplimiento de los principios, deberes y obligaciones que establecen la Ley General, los Lineamientos Generales y la normativa aplicable en materia de protección de datos personales, el Comité de Transparencia supervisará a las Unidades Administrativas para garantizar el derecho a la protección de datos personales de conformidad al artículo 84 fracción 1 de la Ley General.

Artículo 78.- La supervisión en materia de protección de datos personales se sustanciará mediante requerimientos de información sobre el tratamiento de datos personales, así como de sugerencias a las Unidades Administrativas para prevenir algún incumplimiento a las disposiciones en materia de protección de datos personales.

TRANSITORIOS

PRIMERO. - La presente Política entrará en vigor a partir de su aprobación por el Comité de Transparencia.

SEGUNDO. - Notifíquese la presente Política a las personas Titulares de las Unidades Administrativas, difúndase al interior, publíquese en la intranet y en el sitio de Internet.

TERCERO. – El Comité de Transparencia deberá elaborar y coordinar en conjunto con las Unidades Administrativas el Programa de Protección de Datos Personales y ser aprobado por el Comité de Transparencia, a más tardar en seis meses a partir de la entrada en vigor de la presente Política.