ACUERDO mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.

Al margen un logotipo, que dice: Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

CONAIP/SNT/ACUERDO/ORD01-15/12/2017-06

ACUERDO MEDIANTE EL CUAL SE APRUEBAN LAS DISPOSICIONES ADMINISTRATIVAS DE CARÁCTER GENERAL PARA LA ELABORACIÓN, PRESENTACIÓN Y VALORACIÓN DE EVALUACIONES DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES.

Que el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, con fundamento en lo dispuesto por los artículos 10, 12 y 14, fracciones XIX y XX, 74, 76 y quinto transitorio de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 31, fracción I de la Ley General de Transparencia y Acceso a la Información Pública, 10, fracciones II y VII del Reglamento del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales; y el Acuerdo mediante el cual se aprueba la metodología de procesamiento para la estrategia de implementación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, tiene dentro de sus atribuciones las de expedir criterios adicionales para determinar los supuestos en los que se está ante un tratamiento intensivo o relevante de datos personales y disposiciones para la valoración del contenido presentado por los sujetos obligados en la Evaluación de impacto en la protección de datos personales, así como la de emitir acuerdos para dar cumplimiento a las funciones del Sistema Nacional de Transparencia, establecidas en el artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables.

Que en el punto número 8 del Orden del Día, de la Sesión Ordinaria de 2017, del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, celebrada el 15 de diciembre de dos mil diecisiete, fue presentado, sometido a discusión y aprobado por unanimidad el Dictamen que emite la Comisión de Protección de Datos Personales del Sistema Nacional, sobre el Proyecto de Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, en razón de lo anterior, se emite el siguiente:

ACUERDO

PRIMERO.- Se aprueban las Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales conforme al Anexo 1 del Acuerdo CONAIP/SNT/ACUERDO/ORD01-15/12/2017-06

SEGUNDO.- El presente acuerdo entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

TERCERO.- Se instruye al Secretario Ejecutivo a publicar el presente Acuerdo y su Anexo en el Diario Oficial de la Federación, así como en la página del Sistema Nacional de Transparencia, mismos que estarán disponibles para su consulta en el vínculo electrónico siguiente:

http://snt.org.mx/images/Doctos/CONAIP/SNT/ACUERDO/ORD01-15/12/2017-06.pdf

De manera adicional, envíese a las direcciones de correo electrónico institucional de los integrantes del Sistema Nacional, a través de la dirección de correo del Secretario Ejecutivo (federico.guzman@inai.org.mx).

Así lo acordó el Pleno del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en su Sesión Ordinaria de dos mil diecisiete, celebrada el 15 de diciembre del presente año, en la Ciudad de México, lo que se certifica y se hace constar, con fundamento en el artículo 12 fracción XII y 13 fracciones VII y VIII del Reglamento del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.- El Presidente del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, **Francisco Javier Acuña Llamas**.- Rúbrica.- El Secretario Ejecutivo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, **Federico Guzmán Tamayo**.- Rúbrica.

ANEXO 1 DEL ACUERDO CONAIP/SNT/ACUERDO/ORD01-15/12/2017-06

DISPOSICIONES ADMINISTRATIVAS DE CARÁCTER GENERAL PARA LA ELABORACIÓN, PRESENTACIÓN Y VALORACIÓN DE EVALUACIONES DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES

Capítulo I

De las disposiciones generales

Objeto

Artículo 1. Las presentes Disposiciones administrativas tienen por objeto establecer el marco general aplicable en la elaboración, presentación y valoración de las evaluaciones de impacto en la protección de datos personales.

Definiciones

Artículo 2. Además de las definiciones previstas en el artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para los efectos de las presentes Disposiciones administrativas se entenderá por:

I. Disposiciones administrativas: Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, y

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

Ámbito de validez subjetivo

Artículo 3. Son sujetos obligados a cumplir con las presentes Disposiciones administrativas cualquier autoridad, dependencia, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, organismos constitucionales autónomos, tribunales administrativos, fideicomisos y fondos públicos, del orden federal, estatal y municipal, así como partidos políticos que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que, a su juicio y de conformidad con lo dispuesto en la Ley General o las legislaciones estatales en la materia y las presentes Disposiciones administrativas, impliquen un tratamiento intensivo o relevante de datos personales.

Ámbito de validez objetivo

Artículo 4. Las presentes Disposiciones administrativas serán aplicables a la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, a que se refieren los artículos 3, fracción XVI, 74, primer párrafo, 75, 77, 78 y 79 de la Ley General, así como los relativos en las legislaciones estatales en la materia, así como 74, segundo párrafo y 76 del primer ordenamiento señalado en el presente artículo.

Ámbito de validez territorial

Artículo 5. Las presentes Disposiciones administrativas serán aplicables en todo el territorio nacional.

Capítulo II

De la evaluación de impacto en la protección de datos personales

Evaluación de impacto a la protección de datos personales

Artículo 6. La evaluación de impacto en la protección de datos personales es un documento mediante el cual el responsable valora los impactos reales respecto de un tratamiento intensivo o relevante de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes, derechos y demás obligaciones en la materia, de acuerdo con lo dispuesto en el artículo 3, fracción XVI de la Ley General.

Objeto de la evaluación de impacto en la protección de datos personales

Artículo 7. La evaluación de impacto en la protección de datos personales tiene por objeto:

I. Identificar y describir los altos riesgos potenciales y probables que entrañen los tratamientos intensivos o relevantes de datos personales;

II. Describir las acciones concretas para la gestión de los riesgos a que se refiere la fracción anterior del presente artículo;

III. Analizar y facilitar el cumplimiento de los principios, deberes, derechos y demás obligaciones previstas en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables, respecto a tratamientos intensivos o relevantes de datos personales, y

IV. Fomentar una cultura de protección de datos personales al interior de la organización del responsable.

Tratamientos intensivos o relevantes de datos personales de carácter general

Artículo 8. Para efectos de las presentes Disposiciones administrativas y en términos de lo dispuesto en el artículo 75 de la Ley General, el responsable estará en presencia de un tratamiento intensivo o relevante de datos personales cuando concurra alguna las siguientes condiciones:

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

II. Se traten datos personales sensibles a los que se refiere el artículo 3, fracción X de la Ley General o los que correspondan en las legislaciones estatales en la materia, entendidos como aquellos que se refieran a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa mas no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual, y

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

Tratamientos intensivos o relevantes de datos personales de manera particular

Artículo 9. Considerando lo dispuesto en el artículo 76 de la Ley General, se entenderá, de manera enunciativa mas no limitativa, que el responsable está en presencia de un tratamiento intensivo o relevante de datos personales, de manera particular, cuando pretenda:

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

II. Evaluar, monitorear, predecir, describir, clasificar o categorizar la conducta o aspectos análogos de los titulares, a través de la elaboración de perfiles determinados para cualquier finalidad, destinados a producir efectos jurídicos que los vinculen o afecten de manera significativa, especialmente, cuando a partir de dicho tratamiento se establezcan o pudieran establecerse diferencias de trato o un trato discriminatorio económico, social, político, racial, sexual o de cualquier otro tipo que pudiera afectar la dignidad o integridad personal de los titulares;

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

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

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

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

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

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

IX. Realizar transferencias internacionales de datos personales a países que no cuenten en su derecho interno con garantías suficientes y equivalentes para asegurar la debida protección de los datos personales, conforme al sistema jurídico mexicano en la materia;

X. Revertir la disociación de datos personales para la consecución de finalidades determinadas, especialmente si éstas son de carácter intrusivo o invasivo al titular;

XI. Tratar datos personales sensibles con la finalidad de efectuar un tratamiento sistemático y masivo de los mismos;

XII. Realizar una evaluación sistemática y exhaustiva de aspectos propios de las personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para éstas o que les afecten significativamente de modo similar;

XIII. Realizar un tratamiento a gran escala de datos personales sensibles o datos personales relativos a condenas e infracciones penales, o

XIV. La observación sistemática a gran escala de una zona de acceso público.

Obligación de elaborar una evaluación de impacto en la protección de datos personales

Artículo 10. El responsable que pretenda poner en operación o modificar una política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que, a su juicio y de conformidad con lo dispuesto en la Ley General o las legislaciones estatales en la materia, las presentes Disposiciones administrativas y demás normatividad aplicable, implique un tratamiento intensivo o relevante de datos personales deberá elaborar y presentar ante el Instituto o los organismos garantes una evaluación de impacto en la protección de datos personales de conformidad con los citados ordenamientos.

Evaluaciones de impacto en la protección de datos personales interinstitucionales

Artículo 11. Cuando dos o más responsables, de manera conjunta o coordinada, pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que, a su juicio y de conformidad con lo dispuesto en la Ley General o las legislaciones estatales en la materia, las presentes Disposiciones administrativas y demás normatividad aplicable, impliquen un tratamiento intensivo o relevante de datos personales deberán elaborar de manera conjunta una sola evaluación que será presentada al Instituto y/o los organismos garantes conforme a las siguientes reglas:

I. Si los responsables son del orden federal, la presentación de ésta se deberá hacer ante el Instituto;

II. Si los responsables son del orden federal, estatal y/o municipal, la presentación de ésta se deberá hacer ante el Instituto y los organismos garantes competentes;

III. Si los responsables son del orden estatal y/o municipal de una sola entidad federativa, la presentación de ésta se deberá hacer ante el organismo garante de dicha entidad;

IV. Si los responsables son del orden estatal y/o municipal de dos o más entidades federativas, la presentación de ésta se deberá hacer ante los organismos garantes de dichas entidades federativas según corresponda, o

V. Si los responsables son del orden municipal de dos o más entidades federativas, la presentación de ésta se deberá hacer ante los organismos garantes de dichas entidades federativas según corresponda.

A la evaluación de impacto en la protección de datos personales a que se refiere el presente artículo, le resultará aplicable lo dispuesto en el presente Capítulo y los Capítulos III y IV con las particularidades que específicamente se señalen.

Opinión del Instituto y los organismos garantes

Artículo 12. En caso de que el responsable tuviera dudas sobre la obligación de elaborar y presentar una evaluación de impacto en la protección de datos personales respecto al carácter intensivo o relevante de determinado tratamiento de datos personales que pretenda efectuar o modificar, podrá consultar al Instituto o los organismos garantes de acuerdo con lo siguiente:

I. La consulta deberá presentarse en el domicilio del Instituto o de los organismos garantes, o bien, a través de cualquier otro medio que éstos habiliten para tal efecto, previo a la implementación de la política pública, programa, sistema o plataforma informática, aplicaciones electrónicas o cualquier otra tecnología;

II. La consulta deberá describir detalladamente el tratamiento de datos personales que se pretende efectuar o modificar, indicando con especial énfasis el fundamento que lo habilita a tratar los datos personales conforme a la normatividad que le resulte aplicable; las finalidades concretas, lícitas, explícitas y legítimas del tratamiento; el tipo de datos personales, precisando los datos personales sensibles; las categorías de titulares; las transferencias que, en su caso, se realizarían precisando las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales de carácter privado, nacionales y/o internacionales, en su calidad de destinatarios de los datos personales; la tecnología utilizada, así como cualquier otra información relevante para el caso concreto;

III. La consulta deberá incluir el nombre completo, cargo, unidad administrativa de adscripción, correo electrónico y teléfono institucional de la persona designada para proporcionar mayor información y/o documentación al respecto;

IV. La consulta podrá ir acompañada de aquellos documentos que el responsable considere conveniente hacer del conocimiento del Instituto o los organismos garantes;

V. Si el Instituto o los organismos garantes consideran que no cuentan con la suficiente información para emitir su opinión técnica, deberán requerir al responsable, por una sola ocasión y en un plazo que no podrá exceder de cinco días contados a partir del día siguiente de la presentación de la consulta, la información adicional que consideren pertinente;

VI. El responsable contará con un plazo máximo de cinco días, contados a partir del día siguiente de la recepción del requerimiento de información adicional, para proporcionar mayores elementos al Instituto o los organismos garantes con el apercibimiento de que en caso de no cumplir se tendrá por no presentada su consulta;

VII. El requerimiento de información adicional tendrá el efecto de interrumpir el plazo que tiene el Instituto o los organismos garantes para emitir su opinión técnica, por lo que el cómputo de dicho plazo se reanudará a partir del día siguiente de su desahogo, y

VIII. El Instituto o los organismos garantes deberán emitir la opinión técnica para confirmar o negar la obligación del responsable de elaborar y presentar una evaluación de impacto en la protección de datos personales atendiendo al carácter intensivo o relevante del tratamiento de datos personales que pretende poner en operación o modificar en un plazo que no podrá exceder de quince días, contados a partir del día siguiente a la recepción de la consulta, el cual no podrá ampliarse.

Consultas externas

Artículo 13. De manera previa a la presentación de la evaluación de impacto en la protección de datos personales ante el Instituto o los organismos garantes, el responsable podrá llevar a cabo consultas externas con los titulares o público involucrado en la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que pretenda implementar o modificar y que implique un tratamiento intensivo o relevante de datos personales, las cuales deberán ser documentadas.

Capítulo III

Del contenido de las evaluaciones de impacto en la protección de datos personales

Contenido mínimo de las evaluaciones de impacto en la protección de datos personales

Artículo 14. En la evaluación de impacto en la protección de datos personales, el responsable deberá señalar, al menos, la siguiente información:

I. La descripción de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales que pretenda poner en operación o modificar;

II. La justificación de la necesidad de implementar o modificar la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;

III. La representación del ciclo de vida de los datos personales a tratar;

IV. La identificación, análisis y descripción de la gestión de los riesgos inherentes para la protección de los datos personales;

V. El análisis de cumplimiento normativo en materia de protección de datos personales de conformidad con la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables;

VI. Los resultados de la o las consultas externas que, en su caso, se efectúen;

VII. La opinión técnica del oficial de protección de datos personales respecto del tratamiento intensivo o relevante de datos personales que implique la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, en su caso, y

VIII. Cualquier otra información o documentos que considere conveniente hacer del conocimiento del Instituto o los organismos garantes en función de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales y que pretenda poner en operación o modificar.

Descripción de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología

Artículo 15. En la descripción de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales y que pretenda poner en operación o modificar, el responsable deberá indicar, al menos, la siguiente información:

I. Su denominación;

II. El nombre de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;

III. Los objetivos generales y específicos que persigue la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;

IV. El fundamento legal de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, conforme a sus facultades o atribuciones que la normatividad aplicable le confiera;

V. Las categorías de los titulares, distinguiendo aquéllos que pertenezcan a grupos vulnerables en función de su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica;

VI. Los datos personales que serán objeto de tratamiento, distinguiendo, en su caso, los datos personales sensibles;

VII. Las finalidades del tratamiento intensivo o relevante de datos personales;

VIII. Los procesos, fases o actividades operativas de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que involucren el tratamiento de datos personales, así como la descripción puntual de los mismos;

IX. La forma en que se recabarán los datos personales o, en su caso, las fuentes de las cuales provienen;

X. Las transferencias de datos personales que, en su caso, pretendan efectuarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, indicando las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales de carácter privado, nacionales y/o internacionales en su calidad de destinatarios de los datos personales, y las finalidades de estas transferencias;

XI. El tiempo de duración de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, incluyendo aquél que corresponda específicamente al tratamiento intensivo o relevante de datos personales;

XII. La tecnología que se pretende utilizar para efectuar el tratamiento intensivo o relevante de datos personales;

XIII. Las medidas de seguridad de carácter administrativo, físico y técnico a implementar de conformidad con lo previsto en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables;

XIV. El nombre y cargo del servidor o de los servidores públicos que cuentan con facultad expresa para decidir, aprobar o autorizar la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, y

XV. Cualquier otra información o documentos que considere conveniente hacer del conocimiento del Instituto o los organismos garantes.

Contenido adicional para las evaluaciones de impacto en la protección de datos personales interinstitucionales

Artículo 16. Tratándose de una evaluación de impacto en la protección de datos personales interinstitucional, de manera adicional a lo previsto en el artículo anterior, el responsable deberá señalar lo siguiente:

I. La denominación de los responsables conjuntos que presentan la evaluación de impacto en la protección de datos personales;

II. La denominación del responsable líder del proyecto, entendido para efecto de las presentes Disposiciones administrativas como el responsable que tiene a su cargo coordinar las acciones necesarias entre los distintos responsables para la elaboración de la evaluación de impacto en la protección de datos personales, y

III. Las obligaciones, deberes, responsabilidades, límites y demás cuestiones relacionadas con la participación de todos los responsables.

Justificación de la necesidad de implementar o modificar la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología

Artículo 17. En la evaluación de impacto en la protección de datos personales, el responsable deberá señalar las razones o motivos que justifican la necesidad de poner en operación o modificar la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, en función de las atribuciones que la normatividad aplicable le confiera precisando para tal efecto:

I. Si la o las medidas propuestas son susceptibles o idóneas para garantizar el derecho a la protección de datos personales de los titulares;

II. Si la o las medidas propuestas son las estrictamente necesarias, en el sentido de ser las más moderadas para garantizar el derecho a la protección de datos personales de los titulares, y

III. Si la o las medidas son equilibradas en función del mayor número de beneficios o ventajas que perjuicios para el garantizar el derecho a la protección de datos personales de los titulares.

Lo anterior, con la finalidad de que el responsable adopte las medidas menos intrusivas en lo que respecta a la protección de datos personales de los titulares.

Ciclo de vida de los datos personales

Artículo 18. En la evaluación de impacto en la protección de datos personales, el responsable deberá describir y representar cada una de las fases de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, especificando el ciclo de vida de éstos a partir de su obtención, aprovechamiento, explotación, almacenamiento, conservación o cualquier otra operación realizada, hasta la supresión de los mismos.

Además de lo previsto en el párrafo anterior del presente artículo, el responsable deberá señalar:

I. Las fuentes internas y/o externas, así como los medios y procedimientos a través de los cuales se recabarán los datos personales, o bien, son recabados;

II. Las áreas, grupos o personas que llevarán a cabo operaciones específicas de tratamiento con los datos personales;

III. Los plazos de conservación o almacenamiento de los datos personales, y

IV. Las técnicas a utilizar para garantizar el borrado seguro de los datos personales.

Identificación, análisis y gestión de los riesgos para la protección de los datos personales

Artículo 19. En la evaluación de impacto en la protección de datos personales, el responsable deberá incluir la gestión de riesgos que tenga por objeto identificar y analizar los posibles riesgos y amenazas, así como los daños o consecuencias que pudieran producirse o presentarse si llegasen a materializarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.

El responsable deberá presentar un plan general para gestionar los riesgos identificados, en el que se mencione, al menos, lo siguiente:

I. La identificación y descripción específica de los riesgos administrativos, físicos o tecnológicos que podrían presentarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;

II. La ponderación cuantitativa y/o cualitativa de la probabilidad de que los riesgos identificados sucedan, así como su nivel de impacto en los titulares en lo que respecta al tratamiento de sus datos personales, y

III. Las medidas y controles concretos que el responsable adoptará para eliminar, mitigar, transferir o retener los riesgos detectados, de tal manera que no tengan un impacto en la esfera de los titulares, en lo que respecta al tratamiento de sus datos personales.

Análisis de cumplimiento normativo

Artículo 20. En la evaluación de impacto en la protección de datos personales, el responsable deberá señalar los mecanismos o procedimientos que adoptará para que la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que pretende implementar o modificar y que implique un tratamiento intensivo o relevante de datos personales cumpla, por defecto y diseño, con los principios, deberes, derechos y demás obligaciones previstas en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables.

Informe de la consulta externa

Artículo 21. En caso de que el responsable hubiere realizado consultas públicas a que se refiere el artículo 13 de las presentes Disposiciones administrativas, en la evaluación de impacto en la protección de datos personales deberá informar sobre los resultados de la o las consultas externas, distinguiendo las opiniones, puntos de vista y perspectivas del público que, a su juicio, consideró pertinente incorporar en el diseño o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, de aquéllas que no consideró.

Con relación a las opiniones, puntos de vista y perspectivas no consideradas, el responsable deberá señalar las razones o motivos que lo llevaron a tal decisión.

El Instituto y los organismos garantes podrán tener acceso a los documentos recabados durante las consultas externas.

Opinión técnica del oficial de protección de datos personales

Artículo 22. En la evaluación de impacto en la protección de datos personales, el responsable deberá señalar la opinión y consideraciones técnicas del oficial de protección de datos personales respecto del tratamiento intensivo o relevante de datos personales que implica la puesta a disposición o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, en su caso.

Capítulo IV

Del procedimiento de valoración de las evaluaciones de impacto en la protección de datos personales

Presentación de la evaluación de impacto en la protección de datos personales

Artículo 23. El responsable deberá presentar la evaluación de impacto en la protección de datos personales en el domicilio del Instituto o de los organismos garantes, o bien, a través de cualquier otro medio que éstos habiliten para tal efecto, al menos, treinta días anteriores a la fecha en que pretende poner en operación o modificar la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, de acuerdo con lo dispuesto en el artículo 77 de la Ley General o los que correspondan en las legislaciones estatales en la materia.

Acuerdo de admisión o de requerimiento de información

Artículo 24. Una vez presentada la evaluación de impacto en la protección de datos personales ante el Instituto o los organismos garantes, éstos deberán emitir un acuerdo, dentro de los cinco días contados a partir del día siguiente a la recepción de la evaluación, en el cual:

I. Se admita la evaluación de impacto en la protección de datos personales al cumplir con todos los requerimientos a que se refiere el artículo 14 de las presentes Disposiciones administrativas, o

II. Se requiera información al responsable por no actualizarse lo dispuesto en la fracción anterior.

Requerimiento de información

Artículo 25. Si en la evaluación de impacto en la protección de datos personales el responsable no cumple con alguno de los requisitos previstos en el artículo 14 de las presentes Disposiciones administrativas**,** el Instituto o los organismos garantes deberán requerir al responsable, por una sola ocasión y en el plazo previsto en el artículo anterior, la información que subsane las omisiones.

El responsable contará con un plazo máximo de cinco días, contados a partir del día siguiente de la recepción del requerimiento de información, para subsanar las omisiones con el apercibimiento de que en caso de no cumplir se tendrá por no presentada la evaluación de impacto en la protección de datos personales.

El requerimiento de información tendrá el efecto de interrumpir el plazo que tiene el Instituto o los organismos garantes para emitir, en su caso, su dictamen, por lo que se reanudará el cómputo de dicho plazo a partir del día siguiente de su desahogo.

Realización de diligencias y/o reuniones

Artículo 26. El Instituto o los organismos garantes podrán realizar, durante toda la etapa de valoración de una evaluación de impacto en la protección de datos personales, diligencias y/o reuniones de trabajo que considere pertinentes con el responsable, con el objeto de contar con mayores elementos antes de emitir, en su caso, su dictamen.

De toda diligencia o reunión de trabajo celebrada, el Instituto o los organismos garantes deberán levantar un acta en la que harán constar lo siguiente:

I. El lugar, fecha y hora de realización de la diligencia o reunión de trabajo;

II. La denominación del responsable;

III. Los nombres completos y cargos de todos los servidores públicos y personas que intervinieron;

IV. El nombre de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, objeto de la evaluación de impacto en la protección de datos personales, así como las finalidades que motivan el tratamiento de los datos personales;

V. La narración circunstanciada de los hechos ocurridos durante la diligencia o reunión de trabajo, incluyendo los acuerdos alcanzados, y

VI. El nombre completo y firma del servidor público que represente al responsable, al Instituto o los organismos garantes, así como el nombre de cualquier otro asistente.

Valoración de la evaluación de impacto en la protección de datos personales

Artículo 27. El Instituto o los organismos garantes deberán valorar la evaluación de impacto en la protección de datos personales tomando en cuenta lo siguiente:

I. Los objetivos generales y específicos que persigue la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;

II. Las razones o motivos que justifican la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, en función de las atribuciones o facultades del responsable que la normatividad aplicable le confiera;

III. Las categorías de titulares, distinguiendo aquéllos que pertenezcan a grupos vulnerables en función de su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica;

IV. Los datos personales tratados y su volumen;

V. Las finalidades del tratamiento intensivo o relevante de datos personales;

VI. Las transferencias, nacionales o internacionales, de datos personales que, en su caso, pretendan efectuarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;

VII. La tecnología utilizada para efectuar el tratamiento intensivo o relevante de datos personales;

VIII. Las medidas de seguridad de carácter administrativo, físico y técnico que se pretenden adoptar;

IX. Los posibles riesgos y amenazas, así como el daño o consecuencias que pudieran producirse o presentarse si llegasen a materializarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;

X. Las medidas y controles concretos que el responsable adoptará para eliminar, mitigar, transferir o retener los riesgos identificados;

XI. Los mecanismos o procedimientos que adoptará el responsable para que la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales cumpla, desde el diseño y por defecto, con las obligaciones previstas en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables;

XII. La opinión técnica del oficial de protección de datos personales respecto del tratamiento intensivo o relevante de datos personales que implique la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, en su caso, y

XIII. Cualquier otra información que considere pertinente atendiendo a las circunstancias del caso en particular.

Con relación a la fracción X del presente artículo, si durante la valoración de la evaluación de impacto en la protección de datos personales por parte del Instituto o los organismos garantes, el responsable advierte un cambio en los riesgos identificados respecto al tratamiento intensivo o relevante de datos personales, deberá presentar las modificaciones que resulten procedentes a la gestión de riesgos entregada en su momento, en el domicilio del Instituto o de los organismos garantes, o bien, a través de cualquier otro medio que éstos habiliten para tal efecto, de manera inmediata.

Lo anterior, tendrá el efecto de reiniciar el plazo que tiene el Instituto o los organismos garantes para emitir el dictamen en términos de lo dispuesto en la Ley General o las legislaciones estatales en la materia, las presentes Disposiciones administrativas y demás normatividad aplicable.

Sentido del dictamen del Instituto o los organismos garantes

Artículo 28. El Instituto o los organismos garantes deberán emitir un dictamen dentro de los treinta días, contados a partir del día siguiente a la recepción de la evaluación de impacto en la protección de datos personales, en el cual, de manera fundada y motivada, señalará:

I. Que la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales cumple con lo dispuesto en la Ley General o las legislaciones estatales y demás normatividad aplicable, y por lo tanto, no será necesario emitir recomendaciones no vinculantes al respecto, o

II. Que la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales no cumple con lo dispuesto en la Ley General o las legislaciones estatales y demás normatividad aplicable, y por lo tanto, será necesario emitir recomendaciones no vinculantes al respecto.

Alcance del dictamen del Instituto o los organismos garantes

Artículo 29. Tratándose del dictamen a que se refiere el artículo anterior, el Instituto o los organismos garantes deberán pronunciarse sobre la pertinencia de:

I. Los controles y medidas que el responsable adoptará para eliminar, mitigar, transferir o retener los riesgos identificados;

II. Los mecanismos o procedimientos que adoptará el responsable para que la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales cumpla, desde el diseño y por defecto, con las obligaciones previstas en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables, y

III. La puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, en cuanto a la protección que de éstos se refiere.

Aunado a lo previsto en el párrafo anterior del presente artículo, el dictamen emitido por el Instituto o los organismos garantes podrá orientar al responsable para el fortalecimiento y mejor cumplimiento de las obligaciones previstas en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables, señalando medidas, acciones y sugerencias específicas en función de las características generales y particularidades de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.

Efectos de los dictámenes del Instituto y los organismos garantes

Artículo 30. El dictamen del Instituto o de los organismos garantes a que se refiere el artículo anterior no tendrá por efecto:

I. Impedir la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, y

II. Validar el presunto cumplimiento de las obligaciones previstas en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables, en perjuicio de las atribuciones conferidas al Instituto y los organismos garantes.

Lo anterior, dejando a salvo la atribución que tiene el Instituto o los organismos garantes para iniciar, en su momento, procedimientos de verificación respecto a los tratamientos intensivos o relevantes de datos personales que son sometidos a una evaluación de impacto en la protección de datos personales de conformidad con la Ley General, las legislaciones estatales en la materia, las presentes Disposiciones administrativas y demás normatividad aplicable.

Dictámenes sobre evaluaciones de impacto en la protección de datos personales interinstitucionales

Artículo 31. Tratándose de una evaluación de impacto en la protección de datos personales interinstitucional a que se refiere el artículo 11 de las presentes Disposiciones administrativas**,** el Instituto y los organismos garantes deberán emitir su dictamen en función de los procesos de datos personales que estén a cargo del o los responsables que les competa conocer en el ámbito de sus respectivas atribuciones.

Aunado a lo previsto en el párrafo anterior, el Instituto y los organismos garantes podrán llevar a cabo gestiones coordinadas para evitar la emisión de dictámenes contradictorios.

Informe de implementación de las recomendaciones no vinculantes

Artículo 32. El Instituto o los organismos garantes podrán solicitar al responsable que informe sobre la implementación de las recomendaciones no vinculantes emitidas en un plazo máximo de veinte días, contados a partir del día siguiente a la recepción del requerimiento.

Lo anterior, con la finalidad de que el Instituto y los organismos garantes puedan conocer la incidencia de sus recomendaciones no vinculantes en la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales implementada o modificada, en el marco de un proceso de mejora continua de sus procesos relacionadas con las evaluaciones de impacto en la protección de datos personales, o bien, en cumplimiento de otras atribuciones.

Capítulo V

De la exención de la presentación de evaluaciones de impacto en la protección de datos personales

Exención para la presentación de evaluaciones de impacto en la protección de datos personales

Artículo 33. De conformidad con el artículo 79 de la Ley General o los que correspondan en las legislaciones estatales en la materia, el responsable no deberá realizar y presentar una evaluación de impacto en la protección de datos personales cuando pretenda poner en operación o modificar una política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales y a su juicio:

I. Se comprometan los efectos que se pretenden lograr con la posible puesta en operación o modificación de política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, o

II. Se trate de situaciones de emergencia o urgencia.

Presentación y contenido del informe de exención

Artículo 34. Tratándose del artículo anterior el responsable deberá presentar un informe en el domicilio del Instituto o de los organismos garantes, o bien, a través de cualquier otro medio que éstos habiliten para tal efecto durante los primeros treinta días posteriores a la fecha de la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, contados a partir del primer día de la puesta en operación o modificación de ésta, a través del cual, de manera fundada y motivada, señale, al menos, lo siguiente:

I. La denominación y los objetivos generales y específicos que persigue la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;

II. Las finalidades del tratamiento intensivo o relevante de datos personales;

III. Las razones o motivos que le permitieron determinar que la evaluación de impacto en la protección de datos personales compromete los efectos de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales que pretende implementar o modificar, o bien, la situación de emergencia o urgencia que hacen inviable la presentación de ésta;

IV. Las consecuencias negativas que se derivarían de la elaboración y presentación de la evaluación de impacto en la protección de datos personales;

V. El fundamento legal que habilitó el tratamiento de datos personales en el marco de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se pretende poner en operación o modificar;

VI. La fecha en que se puso en operación o modificó la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, así como su periodo de duración;

VII. La opinión técnica del oficial de protección de datos personales respecto del tratamiento intensivo o relevante de datos personales que implique la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, en su caso, y

VIII. Los mecanismos o procedimientos adoptados por el responsable para que la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales cumpla, desde el diseño y por defecto, con todas las obligaciones previstas en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables.

Notificación de admisión o de requerimiento de información

Artículo 35. Una vez presentado el informe ante el Instituto o los organismos garantes, éstos deberán emitir una notificación, dentro de los cinco días contados a partir del día siguiente a la recepción de éste, en la cual:

I. Se tenga por presentado el informe para su valoración, o

II. Se requiera información al responsable por no actualizarse lo dispuesto en la fracción anterior del presente artículo.

Requerimiento de información al responsable sobre el informe

Artículo 36. Si en el informe a que se refiere el presente Capítulo, el responsable no cumple con alguno de los requisitos previstos en el artículo 34, el Instituto o los organismos garantes deberán requerir al responsable, por una sola ocasión y en el plazo previsto en el artículo anterior, la información que subsane las omisiones.

El responsable contará con un plazo máximo de cinco días, contados a partir del día siguiente de la recepción del requerimiento de información, para subsanar las omisiones con el apercibimiento de que en caso de no cumplir se tendrá por no presentado el informe.

El requerimiento de información tendrá el efecto de interrumpir el plazo que tiene el Instituto o los organismos garantes para emitir su respuesta, por lo que se reanudará el cómputo de dicho plazo a partir del día siguiente de su desahogo.

Respuesta del Instituto o los organismos garantes del informe

Artículo 37. El Instituto o los organismos garantes deberán analizar el informe del responsable a que se refiere el presente Capítulo en un plazo máximo de quince días contados a partir del día siguiente de su recepción y emitir una respuesta en los siguientes sentidos:

I. Determinando que la presentación de la evaluación de impacto en la protección de datos personales comprometía los efectos de política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales que se pretender poner en operación o modificar;

II. Reconociendo la situación de emergencia o urgencia planteada por el responsable, o

III. Ordenando la presentación de la evaluación de impacto en la protección de datos personales por no actualizarse los supuestos a que se refieren los artículos 79 de la Ley General o los que correspondan en las legislaciones estatales en la materia y 33 de las presente Disposiciones administrativas ante el Instituto y los organismos garantes, en un plazo máximo de diez días contados a partir del día siguiente de la notificación de la respuesta conforme a lo dispuesto en dicho ordenamiento o las legislaciones estatales en la materia, las presentes Disposiciones administrativas y demás normatividad aplicable.

Transitorios

Único. Las presentes Disposiciones administrativas entrarán en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

(R.- 461459)