Guía para la elaboración de evaluaciones de impacto a la privacidad

Documento orientador en el marco de la Protección de Datos Personales en Posesión de los Particulares

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES
DIRECCIÓN GENERAL DE NORMATIVIDAD Y CONSULTA

Directorio

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

Av. Insurgentes Sur 3211, Insurgentes Cuicuilco,
Alcaldía Coyoacán,
Ciudad de México, C.P 04530 Edición, diciembre de 2020

Contenido

Directorio 2
Abreviaturas 4
Glosario 5
Introducción 6
La EIP como una buena práctica o política 10
Requerimientos de la LFPDPPP aplicables a las EIP 13
¿Qué es una EIP? 16
¿Qué tratamientos pueden 17
¿Cómo realizar una EIP? 19
¿En qué momento debe llevarse a cabo una EIP? 19
¿Qué actores podrían participar en la elaboración de una EIP? 21
¿Cuál es la metodología para llevar a cabo una EIP? 22
Descripción del tratamiento previsto 24
Evaluación de la necesidad y la proporcionalidad 24
Medidas previstas para demostrar la conformidad 25
Evaluación de los riesgos para los derechos y libertades 26
Medidas previstas para afrontar los riesgos 26
Documentación 27
Supervisión y examen 27
¿Existe la obligación de publicar la EIP? 28
¿Puedo consultar al INAI? 28
Preguntas frecuentes 30
Fuentes de referencia 31
Herramientas de facilitación elaboradas por el INAI que podrán ser utilizadas para la EIP 34
Legislación consultada 36

Abreviaturas

CPEUM	Constitución Política de los Estados Unidos Mexicanos.
Directrices EIPD	Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679.
DOF	Diario Oficial de la Federación.
CEPD	Comité Europeo de Protección de Datos.
EIP	Evaluación de Impacto a la Privacidad.
EPDPEI	Estándares de Protección de Datos Personales para los Estados Iberoamericanos.
Guía LFPDPPP	Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
INAI o Instituto	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
LGPDPPSO	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
RGPD	REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
RLFPDPPP	Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Glosario

Alta Dirección: Toda persona con poder legal de toma de decisión en las políticas de la organización.

Consentimiento: Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de estos.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable.

Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

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

Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Transferencia: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.

.

Introducción

La LFPDPPP, publicada en el DOF el 5 de julio de 2010 se caracterizó como un ordenamiento jurídico completo en la materia, en concordancia con las mejores prácticas internacionales.

Sin embargo, la década que sucedió a la entrada en vigor de la LFPDPPP ha resultado especialmente dinámica en el ámbito nacional e internacional, a través de procesos de reforma e integración normativa que han consolidado un marco de referencia robusto para la protección de datos personales en nuestro país.

Así, durante dicho periodo, con la reforma constitucional en materia de transparencia del 7 de febrero de 2014, se inició una nueva época para el entonces denominado Instituto Federal de Acceso a la Información y Protección de Datos, ahora INAI, como organismo constitucionalmente autónomo en materia de transparencia, acceso a la información y protección de datos personales, con atribuciones que se extendieron al ámbito nacional, que a su vez fijó las condiciones para el establecimiento de bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados de los tres niveles de gobierno, a través de la LGPDPPSO, publicada en el DOF el 26 de enero de 2017.

A partir de entonces, el régimen jurídico mexicano de la protección de datos personales cuenta con los elementos para acreditar su conformidad con los estándares de otros países, inclusive con aquellos que cuentan con niveles altos de protección, lo que a su vez permitió, su adhesión al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, Francia, abierto a firma el 28 de enero de 1981, denominado Convenio 108, así como, su Protocolo Adicional, abierto a firma el 8 de noviembre del año 2001, instrumentos que entraron en vigor en nuestro país a partir del 1 de octubre de 2018, en términos del artículo transitorio único de sendos Decretos publicados en el DOF el 28 de septiembre del año de referencia.

Lo anterior, mientras que en el plano internacional se consolidó el modelo europeo a través de la publicación y entrada en vigor del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, también denominado, Reglamento General de Protección de Datos, instrumento normativo que constituye la principal referencia de las instituciones jurídicas vinculadas con la protección de datos personales a nivel internacional.

Adicionalmente, conviene señalar que, a partir del 10 de octubre de 2018, se abrió a firma el Protocolo que modifica el Convenio para la Protección de las Personas

con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108), registrado con el número 223, al que se le ha denominado Convenio 108+ o Convenio 108 modernizado.

En el ámbito regional, reconociendo que los Estados Iberoamericanos están obligados a adoptar un régimen que garantice a los titulares una serie de mecanismos y procedimientos para presentar sus reclamaciones ante la autoridad de control cuando consideren vulnerado su derecho a la protección de datos personales, así como para ser indemnizados cuando hubieren sufrido daños y perjuicios como consecuencia de una violación de su derecho, y, destacando la importancia de establecer una base mínima para la cooperación internacional entre las autoridades de control latinoamericanas y entre éstas y las de terceros países, con la finalidad de favorecer y facilitar la aplicación de la legislación en la materia y una protección efectiva de los titulares, la Red Iberoamericana de Protección de Datos Personales, en cuyos trabajos participa con el carácter de miembro el INAI, el 20 de junio de 2017, determinó adoptar los EPDPEI, para que con el carácter de directrices orientadoras contribuyan a la emisión de iniciativas regulatorias de protección de datos personales en la región de los países que aún no cuentan con estos ordenamientos, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes, favoreciendo la adopción de un marco regulatorio armonizado que ofrezca un nivel adecuado de protección de las personas físicas respecto al tratamiento de sus datos personales y garantizando, a su vez, el desarrollo comercial y económico de la región.

Finalmente, otro factor a considerar es la integración de México dentro del entorno económico internacional, así como en la creciente economía digital, supuestos que provocan de facto que el régimen jurídico mexicano de la protección de datos personales deba adaptarse a las necesidades de las relaciones comerciales que tiene nuestro país con los diversos mercados regionales e internacionales, en los cuales, la protección de datos personales adquiere cada vez mayor importancia dentro de los entornos digitales y el comercio electrónico, como un requisito a cubrir a fin de evitar que dicha materia se convierta en una barrera no arancelaria para las relaciones internacionales.

Bajo este contexto, es posible advertir que, si bien los cambios producidos en el periodo de referencia resultan relevantes, el adecuado diseño normativo de la LFPDPPP permitió que dicho instrumento se haya mantenido vigente[1] frente a estos nuevos y variados escenarios.

Ahora bien, las evaluaciones de impacto en la protección de datos personales constituyen herramientas que permiten implementar un enfoque de privacidad por diseño, en concordancia con las mejores prácticas internacionales, por lo que,

[1] No obstante, a fin de contar con un marco legislativo y normativo adecuado en materia de protección de datos personales en po sesión de los particulares, atendiendo los diversos criterios judiciales y jurisprudenciales que han surgido con motivo de su aplicación, la reforma a la LFPDPPP y a su Reglamento resultaría deseable para acreditar una conformidad plena del régimen jurídico mexicano en materia de protección de datos personales..

el presente documento no tiene carácter mandatorio, sino orientador, a fin de proporcionar apoyo técnico a los responsables, difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana y promover su ejercicio, a través de una serie de recomendaciones basadas en estándares y mejores prácticas internacionales en materia de seguridad de la información, que pudieran resultar aplicables en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas de los responsables, de conformidad con lo previsto por los artículos 38 y 39, fracciones III, IV y V, de la LFPDPPP.

A manera de ejemplo, se considera pertinente señalar que entidades como la Organización Internacional de Estandarización, con la ISO/IEC29134:2017, relativa adirectrices para evaluaciones de impacto a la privacidad, como parte de las técnicas de seguridad de tecnologías de la información; constituyen muestras de los esfuerzos generados en el sector privado para la implementación de estas evaluaciones, como una herramienta preventiva que coadyuve en la gestión de la seguridad por parte de las entidades y organizaciones. Asimismo, a nivel internacional se han identificado distintas ventajas y oportunidades a partir de la implementación de este tipo de evaluaciones por parte de los responsables del tratamiento de datos personales , tales como las que se encuentran referidas en el estudio denominado “The state of the art in privacy impact assessment” en el cual se proporcionan antecedentes, identifican beneficios y se analizan los elementos que pueden ser utilizados para la construcción de una metodología sobre la figura de evaluación de impacto a la privacidad.

En consecuencia, se considera factible y viable que los responsables del tratamiento de datos personales en posesión de los particulares puedan incorporar dentro de su actuación, como una buena práctica, la realización de una EIP previo a llevar a cabo un nuevo tratamiento de datos o una modificación sustancial a un tratamiento ya existente.

En este sentido, y con relación a la adopción de buenas prácticas de conformidad con lo previsto en el artículo 80, fracción VIII, del RLFPDPPP, la realización de una EIP podrá configurarse como una medida adoptada por los responsables con el objetivo de promover su compromiso con la rendición de cuentas y adopción de políticas internas consistentes con criterios externos, así como para auspiciar mecanismos para implementar políticas de privacidad, incluyendo las evaluaciones de riesgo.

Asimismo, y de conformidad con las obligaciones que establece el cumplimiento del principio de responsabilidad, existen una serie de medidas que los responsables podrán adoptar, previstas en el artículo 48 del RLFPDPPP, por lo que, la elaboración de una EIP podrá traducirse para el responsable que decida incorporarla, en términos de la fracción V del precepto legal señalado, en una medida para instrumentar un procedimiento para atender el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.

A su vez, con la finalidad de orientar a los responsables y dotar de estructura y contenido a la EIP, se adoptan como referencia las Directrices EIPD, emitidas por el Grupo "Protección de Datos Personales" del artículo 29, el cual se creó de conformidad con el artículo 29 de la Directiva 95/46/CE, órgano consultivo independiente de la Unión Europea en materia de protección de datos y privacidad, el cual se mantuvo durante el periodo transitorio de entrada en vigor del Reglamento antes señalado, que comprendió dos años.

Es decir, con la finalidad de que los responsables que determinen como una buena práctica implementar una EIP, deberían tomar en consideración las disposiciones, herramientas y metodologías que se ajusten a sus necesidades, conforme a los elementos normativos que se señalan en el presente documento, tomando como punto de partida, las Directrices EIPD antes mencionadas, por constituir un marco de referencia sólido de uso extendido en la actualidad. A partir de ello, podrá identificarse el alcance o vinculación de las técnicas y/o metodologías adoptadas que más convengan al responsable conforme a las características de tratamiento que le correspondan.

Finalmente, se determina el alcance o utilidad de la implementación de la EIP en el marco de la LFPDPPP y del contexto previamente establecido, a fin de que una vez que haya sido realizada por el responsable, derivado de los resultados, en caso de que existan dudas se consulte al INAI para que en ejercicio de sus atribuciones de apoyo técnico y de emisión de criterios y recomendaciones, previstas en el artículo 39, fracciones III y IV, de la LFPDPPP a través de la unidad administrativa correspondiente, pueda orientarlos para el cumplimiento de sus obligaciones en materia de protección de datos personales.

Atendiendo lo anterior, se presentan los tramos de control que guardan correspondencia con el flujo identificado en las Directrices EIPD que se toman como referencia, y que, puede esquematizarse de la manera siguiente:

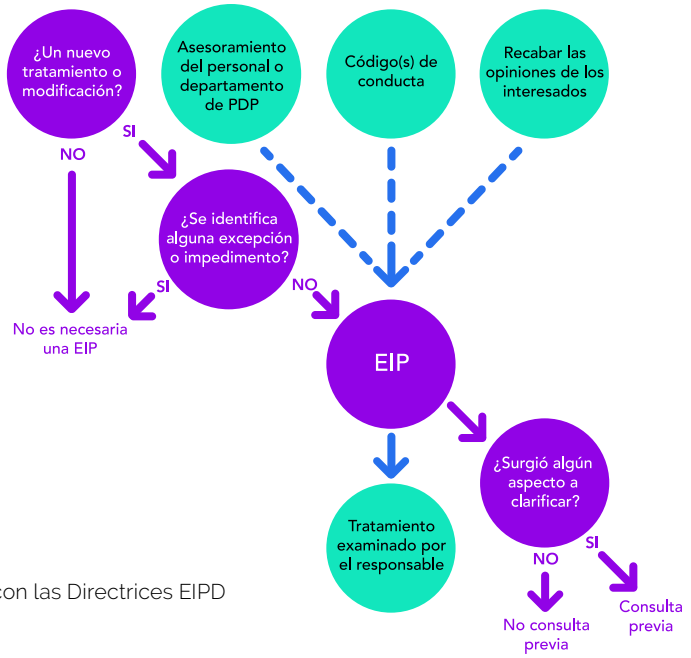

Figura 1.
Flujo de EIP de conformidad con las Directrices EIPD

Para llevar a cabo dichas actividades, la presente guía comienza con un contexto general sobre las EIP, y, posteriormente, relaciona los elementos normativos en materia de protección de datos personales en posesión de los particulares.

Bajo la premisa anterior, se desarrolla de manera enunciativa y únicamente a manera de referencia de implementación, los elementos que deberían considerarse en el marco de la elaboración de una EIP, así como las herramientas que el INAI ha generado a fin de que los responsables puedan considerarlas para efectos de dicho ejercicio.

Complementa el contenido del presente documento, la relación de las principales herramientas que pudieran implementarse en las etapas asociadas a una EIP, así como un listado de fuentes de referencia que pudiera resultar de interés para el responsable que encontrará valor con su elaboración, en el entendido que, cada vez con mayor frecuencia, la adopción de nuevos tratamientos o su modificación basados en nuevas tecnologías, entraña riesgos y dudas que deberían ser atendidos de manera previa al inicio de las operaciones, a fin de disminuir al máximo los riesgos inherentes y privilegiar la privacidad de las y los usuarios por defecto.

Consideraciones anteriores que se comparten a fin de brindar contexto sobre el alcance y estructura del presente documento, esperando que los responsables que acudan al uso de esta guía encuentren un instrumento útil para la debida protección de datos personales y el debido cuidado de la privacidad de sus usuarios, a fin de privilegiar, como buena práctica, un enfoque de privacidad por diseño y de una responsabilidad proactiva.

La EIP como una buena práctica o política

Con el objeto de que los responsables puedan obtener beneficios de la implementación de EIP o de alcanzar resultados en el marco de su esquema de protección e inclusive dentro de sus sistemas de gestión, se recomienda que su implementación obedezca a una decisión estratégica que tome como referencia alguna de las mejores prácticas en la materia en la actualidad.

Para familiarizarse con el uso de dichas herramientas, los responsables podrán tomar como referencia inicial el contenido de la presente guía; asimismo, considerando que la EIP podrá no solo involucrar el derecho a la protección de datos personales, sino incidir sobre otros aspectos relacionados con la privacidad de las personas, se considera importante, cuando proceda y sea del interés del responsable, determinar dentro de los objetivos de la evaluación de impacto los supuestos que ésta podrá abarcar, así como valorar las herramientas a implementar y acreditar medidas de cumplimiento sobre particular.

A fin de determinar algunos elementos importantes para la elaboración de una EIP, conviene que el responsable tenga identificado lo siguiente:

Roles en la organización.

Pueden existir al interior de la organización del responsable distintas áreas que podrían estar involucradas en su desarrollo, como se ejemplifica a continuación:

- La elaboración de la EIP debería corresponder al área o persona líder y/o encargada de la implementación del proyecto, al constituir la principal interesada en el cumplimiento de la conformidad de los requisitos asociados a su implementación.
- La autorización y seguimiento de actividades que se determinen en el plan derivado de la elaboración de la EIP correspondería a la Alta Dirección o al Titular de la organización, o los mecanismos que tenga reconocidos para el seguimiento.
- La asesoría y apoyo técnico al interior de la organización quedaría a cargo de la persona o departamento de protección de datos, así como, en su caso, de la persona o área que desarrolle funciones de seguridad, ya sea de la misma organización o bien, una persona física o moral contratada para tal fin, según corresponda, en términos de los artículos 30 de la LFPDPPP y 59 del RLFPDPPP, respectivamente.

Identificación del contexto de tratamiento y elementos normativos

Se sugiere que la organización realice previamente a una EIP, un análisis del contexto del tratamiento y su vinculación con los elementos normativos, a fin de confirmar si el tiempo, recursos y esfuerzos dedicados a esta herramienta se justifican en función de los resultados esperados o inclusive de las propias circunstancias vinculadas con el tratamiento de datos personales.

Claridad en la identificación de la población objetivo o áreas de enfoque

Generalmente, las EIP se realizan por los responsables para evaluar los efectos potenciales que tendrá la implementación del respectivo tratamiento de datos personales en la población usuaria, sin embargo, pueden existir pluralidad de agentes, requisitos regulatorios o inclusive diversos roles en función de los actores involucrados con el tratamiento de datos personales, así como en su caso, diferentes regímenes de tratamiento (público-privado), diversas jurisdicciones, o, criterios de entes reguladores, como el INAI, con independencia de las instancias revisoras en materia contenciosa, e inclusive, las propias expectativas a generarse por el público en general; supuestos que se sugiere deben quedar delimitados de manera previa a su desarrollo, con la finalidad de que la elaboración de esta herramienta pueda aportar información de valor.

Integración con las demás medidas de seguridad, selección y exclusión de etapas

Tal como se señala a lo largo del documento, existen diversas alternativas para elaborar una EIP, lo cual, permite que el responsable de su elaboración pueda

elegir no sólo una alternativa en concreto, sino que pueda complementarla o ajustarla en función de sus propias necesidades, agregando o eliminando etapas y actividades; sin embargo, cualquier alternativa que se elija deberá implementarse en congruencia con mecanismos y las medidas de seguridad que correspondan en cumplimiento del principio de responsabilidad y el deber de seguridad previstos por la LFPDPPP.

En consecuencia, se sugiere considerar una EIP como un proceso que no se limita a la elaboración de un reporte, sino que debería ser contemplada desde las etapas tempranas de planeación del proyecto mismo, e inclusive, podría mantenerse su implementación aún después del inicio de operaciones del proyecto y durante su ciclo de vida, en el entendido de que nuevos riesgos pudieran surgir conforme el proyecto avance o escale. Para tales efectos, el responsable debería valorar la existencia de otros mecanismos de seguridad que pudieran ser implementados con posterioridad al cierre de la EIP.

Si bien, se identifican diversas metodologías y procesos para la elaboración de una EIP, en función de elementos variados, se considera que pudiera resultar de utilidad al responsable de su elaboración, las principales actividades o etapas que pudieran ser incluidas como parte del proceso de su elaboración, a saber:

- Determinar el contexto del tratamiento y confirmar si resulta necesario elaborar una EIP.
- Identificar el equipo involucrado en su elaboración y ejecución, así como definir términos de referencia.
- Descripción del objetivo o finalidad de la EIP y la identificación de los actores involucrados.
- Análisis de los flujos de información y sus impactos en la privacidad, u otras circunstancias relevantes advertidas en el marco del tratamiento.
- Consultas con los actores involucrados.
- Identificación de riesgos, su administración y en su caso, soluciones propuestas.
- Formulación de recomendaciones y/o determinación de plan de acción.
- Preparación y publicación del reporte por el que se den a conocer los resultados de la EIP.
- Mecanismos de monitoreo y seguimiento de implementación de las recomendaciones, así como para la medición de su eficacia, y en su caso, establecimiento de planes de reacción ante resultados negativos.
- Revisión por terceras partes o mecanismos de auditoría.
- Actualización de la EIP en caso de que se presenten actualizaciones del proyecto.
- Mecanismos de tratamiento para la formulación de consulta ante la autoridad de control.

Requerimientos de la LFPDPPP aplicables a las EIP

El artículo 39 de la LFPDPPP, fracción X, establece que el INAI tiene como atribución elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes.

A su vez, las modificaciones sustanciales representan eventos que se vinculan con cambios en las medidas de seguridad, derivadas de un cambio en el nivel de riesgo conforme lo establece el artículo 62, fracción II, del RLFPDPPP.

Si bien, en términos de las disposiciones antes señaladas, se identifican los elementos básicos que justificarían la elaboración de un estudio de impacto por parte del INAI, con relación a la elaboración como buena práctica de una EIP, por parte de los responsables, se considera de utilidad, tomar como referencia los EPDPEI en su numeral 41, relativo a evaluaciones de impacto a la protección de datos personales.

Sobre el particular, se establece que cuando el responsable pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, realizará de manera previa a la implementación de este, una evaluación de impacto a la protección de los datos personales.

Para tales efectos, la legislación nacional de los Estados Iberoamericanos señala los tratamientos que requieran de una evaluación de impacto a la protección de datos personales; el contenido de éstas, los supuestos en que resulte procedente presentar el resultado ante la autoridad de control, así como los requerimientos de dicha presentación, entre otras cuestiones.

Conforme lo anterior es dable considerar que una EIP procede de manera previa a:

- La puesta en práctica de una nueva modalidad de tratamiento de datos personales.
- La realización de modificaciones sustanciales en tratamientos ya existentes.

Al estar vinculados ambos supuestos con lo previsto por el artículo 62, fracción II, del RLFPPPP, a su vez puede considerarse que esos supuestos deben estar asociados a cambios significativos en el nivel de riesgo, y, por ende, dentro de dicho supuesto se encontrarían comprendidas las hipótesis siguientes:

- Un tratamiento de datos personales que, por su naturaleza, sea probable que entrañe un alto riesgo.
- Un tratamiento de datos personales que, por su alcance, sea probable que

entrañe un alto riesgo.
- Un tratamiento de datos personales que, por su contexto, sea probable que entrañe un alto riesgo.
- Un tratamiento de datos personales que, por sus finalidades, sea probable que entrañe un alto riesgo.

Luego entonces, al clarificar los supuestos y tipos de tratamientos que sean probables que entrañen un alto riesgo, o, produzca cambios significativos en el nivel de riesgo, se advierte que los supuestos de procedencia de una EIP serían los siguientes:

- La puesta en práctica de una nueva modalidad de tratamiento de datos personales que, por su naturaleza, sea probable que entrañe un alto riesgo.
- La puesta en práctica de una nueva modalidad de tratamiento de datos personales que, por su alcance, sea probable que entrañe un alto riesgo.
- La puesta en práctica de una nueva modalidad de tratamiento de datos personales que, por su contexto, sea probable que entrañe un alto riesgo.
- La puesta en práctica de una nueva modalidad de tratamiento de datos personales, que, por sus finalidades, sea probable que entrañe un alto riesgo.
- La realización de modificaciones sustanciales en tratamientos ya existentes que, por su naturaleza, sea probable que entrañe un alto riesgo.
- La realización de modificaciones sustanciales en tratamientos ya existentes que, por su alcance, sea probable que entrañe un alto riesgo.
- La realización de modificaciones sustanciales en tratamientos ya existentes que, por su contexto, sea probable que entrañe un alto riesgo.
- La realización de modificaciones sustanciales en tratamientos ya existentes que, por sus finalidades, sea probable que entrañe un alto riesgo.

Supuestos que, de actualizarse en un caso particular, resultaría recomendable para los responsables la elaboración de una EIP, en función de las consecuencias que pudieran derivar de una inadecuada gestión de riesgos. Al respecto, es importante señalar que la gestión de riesgos forma parte de las acciones que para el cumplimiento del deber de seguridad deberán analizar los responsables.

Con el objeto de identificar los supuestos que podrían estar comprendidos dentro de los casos anteriores, se señala a manera de referencia lo siguiente:

Tratamientos de datos personales que, por su naturaleza, sea probable que entrañe un alto riesgo.

La LFPDPPP previene disposiciones generales en torno al tratamiento de datos personales, así como supuestos especiales que tienen una naturaleza diversa, entre los cuales pudieran estar comprendidos:

Datos personales sensibles, entendidos en términos del artículo 3, fracción VI de la LFPDPPP, aquellos datos personales que afecten a la esfera más íntima de su

titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Menores de edad, personas en estado de interdicción o incapacidad, que en términos de lo previsto por el artículo 89, último párrafo, del RLFPDPPP, existe una previsión especial para el ejercicio de sus derechos ARCO, así como numeral cuarto del Anexo "Buenas prácticas en el aviso de privacidad" de los Lineamientos del Aviso de Privacidad, el responsable podrá informar en el aviso de privacidad las acciones, medidas y previsiones especiales que caractericen este tipo de tratamiento y que lleve a cabo el responsable, a fin de salvaguardar el derecho a la protección de datos personales de estos grupos de personas, lo cual conlleva a su vez, mecanismos de control diferenciados.

Transferencias, las cuales constituyen un tipo de tratamiento de datos personales sujeto a las previsiones del Capítulo V, de la LFPDPPP y Capítulo IV, del RLFPDPPP.

Tratamientos de datos personales que, por su alcance, sea probable que entrañe un alto riesgo.

A fin de dar contenido al concepto de alcance, se advierte que dichos supuestos son susceptibles de vincularse, en función del análisis de factores que en términos del artículo 60 del RLFPDPPP los responsables deberán realizar para determinar la implementación de medidas de seguridad, por lo que, de identificarse la actualización de dos o más factores de riesgo podría configurarse la probable existencia de un riesgo elevado en el tratamiento que se esté analizando.

Tratamientos de datos personales que, por su contexto, sea probable que entrañe un alto riesgo.

Supuestos entre los cuáles se advierte que, como factores a considerar como parte del contexto del tratamiento, podemos identificar los siguientes:

Tratamiento de datos patrimoniales o financieros, que se identifican de manera particular por el artículo 8, párrafo cuarto, de la LFPDPPP, y que representan un alto riesgo, por los incentivos que generan los beneficios potenciales derivados de su obtención por personas no autorizadas.

Probabilidad de ocurrencia de vulneraciones de seguridad, que afecten de forma significativa los derechos patrimoniales o morales de los titulares conforme lo establece el artículo 20 de la LFPDPPP.

Implementación de nuevos productos, servicios, tecnologías y modelos de negocios, al constituir un riesgo identificado expresamente en el artículo 48, fracción V,

del RLFPDPPP, que obliga a instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales.

Tratamientos de datos personales que, por sus finalidades, sea probable que entrañe un alto riesgo.

En este último apartado, conviene señalar que pueden considerarse como supuestos relacionados con un alto riesgo, en función de la finalidad del tratamiento, la identificación de la hipótesis del artículo 112 del RLFPDPPP, relativo al tratamiento de datos personales en la toma de decisiones sin intervención de la valoración humana, que pudiera dar lugar a discriminación, el responsable deberá informar al titular que esta situación ocurre. Así como de lo establecido en el artículo 52 del RLFPDPPP respecto al tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera mediante condiciones o cláusulas de contratación.

¿Qué es una EIP?

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas, el responsable del tratamiento como buena práctica, podrá realizar, antes del tratamiento, una EIP.

Si bien, la normativa aplicable al sector privado no prevé como tal el concepto de lo que es una EIP, se tomará como referencia lo señalado en las Directrices EIPD de conformidad con lo indicado en el marco de referencia antes expuesto.

Por lo tanto, de conformidad con lo previsto en las Directrices EIPD, una EIP pudiera considerarse como:

> *"un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales evaluándolos y determinando las medidas para abordarlos".*

Por tanto, para efectos del presente documento orientador, una EIP es un instrumento de carácter preventivo de gran importancia, no sólo para permitir que los responsables cumplan con las obligaciones establecidas en la LFPDPPP y demás normativa aplicable, sino también para reforzar y demostrar que se han tomado medidas adecuadas para garantizar su aplicación y cumplimiento, tal como lo establece el principio de responsabilidad en los artículos 14 de la LFPDPPP y 47 del RLFPDPPP.

Conforme a las Directrices EIPD, existen diferentes supuestos para la utilización de las EIP:

1. Utilizar una EIP para una única operación de tratamiento de datos.

2. Utilizar una EIP para abordar una serie de operaciones de tratamientos similares que entrañen altos riesgos análogos, por ejemplo, en el supuesto de que varios responsables actualicen una aplicación o un entorno de un tratamiento común.

3. Utilizar una única EIP para evaluar múltiples operaciones de tratamiento que sean similares en términos de naturaleza, alcance, contexto, fines y riesgos. Este puede ser el caso cuando se utiliza tecnología similar para recopilar el mismo tipo de datos para los mismos fines o a operaciones de tratamiento similares aplicadas por varios responsables los cuales deberán compartir o hacer pública una misma EIP de referencia que establezca justificación de porque la realización de solo una.

4. Utilizar una EIP para evaluar un producto tecnológico que sea probable que distintos responsables lo utilicen para realizar diferentes operaciones de tratamiento. En este caso, el responsable del tratamiento que instala el producto tendrá la obligación de llevar a cabo su propia EIP relativa a la aplicación específica, no obstante, este puede basarse en una EIP preparada por el proveedor del producto, sin perjuicio de poner en peligro secretos o riesgos de seguridad al revelar posibles vulnerabilidades

¿Qué tratamientos pueden someterse?

La legislación mexicana no contiene disposiciones expresas respecto de supuestos de tratamientos de datos personales en los que sea necesaria la aplicación de una EIP, sin embargo, atendiendo a las Directrices EIPD y tomándolas como marco orientador, el responsable podría tomar en cuenta los siguientes criterios en ellas contenidos:

- **Evaluación o puntuación:** Cuando el tratamiento conlleve la elaboración de perfiles, especialmente de aspectos relacionados con el rendimiento laboral, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos de los titulares.

- **Toma de decisiones automatizada con efecto jurídico significativo o similar:** Cuando el tratamiento se vea destinado a tomar decisiones sobre los titulares que produce efectos jurídicos para las personas o que les afectan significativamente de modo similar.

- **Observación sistemática:** Cuando el tratamiento sea usado para observar, supervisar y controlar a los titulares, incluidos los datos obtenidos a través de redes o de la observación sistemática de una zona de acceso público.

Este tipo de observación representa un criterio porque los datos personales pueden ser recogidos en circunstancias en las que los titulares pueden no ser conscientes de quién está recopilando sus datos y cómo se usarán. Además, puede resultar imposible para las personas, evitar ser objeto de este tipo de tratamientos en espacios públicos.

• **Datos sensibles:** Cuando el tratamiento involucre datos personales de categorías especiales, como los datos personales sensibles que puedan afectar a la esfera más íntima de su titular, o cuya utilización pueda dar origen a discriminación o conlleve un riesgo grave para éste.

• **Tratamiento de datos a gran escala:** Se determina al considerar el número de titulares afectados, bien como cifra concreta o como proporción de la población correspondiente; el volumen de datos o la variedad de elementos de datos distintos que se procesan; la duración o permanencia de la actividad de tratamiento de datos y el alcance geográfico de la actividad de tratamiento.

• **Asociación o combinación de conjuntos de datos:** Cuando los datos deriven de dos o más operaciones de tratamiento de datos realizadas para distintos fines o por responsables distintos, de manera que exceda las expectativas razonables del titular.

• **Datos relativos a titulares vulnerables:** Cuando el tratamiento de este tipo de datos represente el aumento del desequilibrio de poder entre los titulares y el responsable del tratamiento, lo cual implica que las personas pueden ser incapaces de autorizar o denegar el tratamiento de sus datos, o de ejercer sus derechos. Entre los titulares vulnerables pueden incluirse a niños, empleados, segmentos más vulnerables de la población que necesitan una especial protección o cualquier otro caso en el que se identifique este supuesto.

• **Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas:** Cuando el tratamiento conlleve el uso de una nueva tecnología, toda vez que este nuevo uso puede implicar nuevas formas de recolección y utilización de datos, posiblemente con un alto riesgo para los derechos y libertades de las personas, por lo que las consecuencias personales y sociales del empleo de una nueva tecnología pueden ser desconocidas.

• **Cuando el propio tratamiento impida a los titulares ejercer un derecho o utilizar un servicio o ejecutar un contrato:** Esto incluye operaciones de tratamiento destinadas a permitir, modificar o denegar el acceso de los titulares a un servicio o a un contrato.

Se considera que cuantos más criterios cumpla el tratamiento, más probable será que represente un alto riesgo para los derechos y libertades de los titulares y, por tanto, requiera una EIP independientemente de las medidas que el responsable contemple adoptar.

¿Cómo realizar una EIP?

¿En qué momento debe llevarse a cabo una EIP?

Antes del tratamiento

La EIP debe de realizarse previo a iniciar las operaciones para el tratamiento de datos personales, para que sea posible adoptar medidas para la mitigación, prevención y gestión de posibles riesgos para los derechos y libertades de los titulares de los datos. Lo anterior es así, puesto que es considerada como una herramienta de carácter preventivo y que por consiguiente permitiría tomar decisiones relativas al tratamiento de datos personales que está por llevarse a cabo dentro de las operaciones de cualquier responsable, por lo que, resulta conveniente iniciarse en cuanto se tenga definido el procedimiento a través del cual se realizará el tratamiento de datos, incluso aunque algunos aspectos operacionales de dicho tratamiento no se conozcan aún.

La EIP, deberá de cumplir con su debida actualización a lo largo del ciclo de vida de los datos, lo cual garantizará que se tenga en cuenta la protección de los datos y la confidencialidad de estos, atendiendo siempre la normatividad vigente, pues dicha evaluación debe de verse como un proceso continuo, sobre todo cuando una operación de tratamiento es dinámica y está sujeta a cambios permanentes. En concatenación a esto, resulta necesario repetir pasos concretos de la evaluación a medida que avance el proceso de desarrollo debido a que la selección de determinadas medidas técnicas u organizativas puede afectar a la gravedad o probabilidad de los riesgos que suponga el tratamiento.

Si bien es cierto que la aplicación de esta herramienta debe de realizarse antes del tratamiento de la información, también es cierto que se puede llevar a cabo con posterioridad con motivo de algún cambio en el tratamiento.

En este mismo sentido, la EIP es un proceso que no se agota una vez realizada, sino que implica un proceso de continua revisión, por lo que, cuando en una operación iniciada en la que se haya realizado una EIP, se hayan producido cambios en los riesgos que el tratamiento implica respecto al momento en que el tratamiento se puso en marcha se deberá realizar nuevamente una EIP. Este cambio en los riesgos puede derivar, entre otras causas, del hecho de que se hayan empezado a aplicar nuevas tecnologías a ese tratamiento, de que los datos se estén usando para finalidades distintas o adicionales a las que se decidieron en su momento, o de que se estén obteniendo más datos, o datos diferentes, de los que en principio se utilizaban para el tratamiento.

La EIP, constituye una herramienta útil para los responsables que, en su caso, decidan implementarla como buena práctica, puesto que, con su realización se podrán identificar acciones necesarias que permitan construir el camino para el cumplimiento de los principios de licitud, calidad, lealtad y responsabilidad, los cuales se encuentran establecidos en los artículos 6, 7, 11 y 14 de la LFPDPPP y, 10, 36, 44 y 47 del RLFPDPPP.

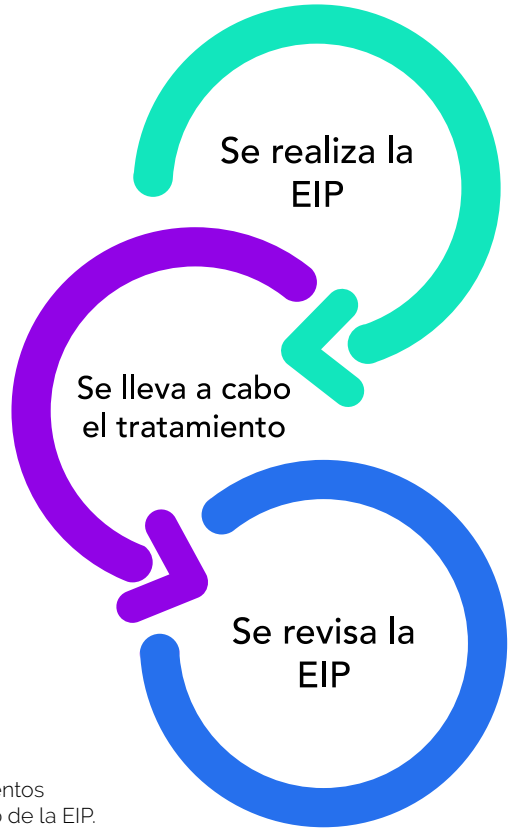

Figura 2.
Proceso general de los momentos relacionados con el desarrollo de la EIP.

Esto debido a que, con la aplicación de la EIP, se pretende establecer que el tratamiento de datos respectivo sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional, lo cual le daría presencia al principio de licitud. Por otro lado, en cuanto al principio de calidad, el responsable tiene la obligación de adoptar los mecanismos que considere necesarios para procurar que los datos personales que vaya a tratar sean exactos, completos, pertinentes, correctos y actualizados, con el fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación.

Asimismo, al aplicar dicha herramienta, se podrá privilegiar la protección de los intereses del titular y la expectativa razonable de privacidad, tal y como lo mandata el principio de lealtad. Por último, el responsable que aplique dicha EIP habrá comenzado su obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado, cumpliendo así con el principio de responsabilidad. Teniendo la oportunidad para ello, de valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines.

¿Qué actores podrían participar en la elaboración de una EIP?

El responsable, junto con la persona o departamento de protección de datos personales asignado por este, y el departamento de seguridad y los encargados del tratamiento.

Corresponde a los responsables del tratamiento que decidan implementar una EIP, como buena práctica, garantizar su elaboración como parte de las medidas a implementar para garantizar el debido tratamiento y cumplir con los principios y obligaciones que establece la LFPDPPP y su RLFPDPPP.

Ahora bien, es de señalar que conforme a lo previsto en el artículo 30 de la LFPDPPP y 59 de su RLFPDPPP, el responsable deberá contar con una persona o departamento de protección de datos personales asignado por el mismo, así como con una persona o un área encargada de la seguridad, ya sea de la misma organización o bien, una persona física o moral contratada para tal fin.

En este sentido, en función de los roles que fueron señalados, dichas áreas participarán en el desarrollo de la EIP, la cual será elaborada por el área o persona líder y/o encargada de la implementación del proyecto para ser ejecutada o autorizada por la Alta Dirección o el Titular de la organización, con la asesoría y apoyo técnico del departamento de datos y de quien desarrolle las funciones de seguridad. Lo anterior, en el entendido de que el desarrollo de una EIP requiere la adecuada involucración de aquellas áreas que tienen un conocimiento profundo del tratamiento.

Si se actualiza el caso de que hubiese un encargado y este lleva a cabo el tratamiento total o parcialmente, el responsable podrá apoyarse de este para realizar la EIP y obtener la información necesaria para su desarrollo.

Resulta una buena práctica que el responsable recabe la opinión de los titulares interesados sobre la operación del tratamiento previsto, siempre que se garantice que el responsable dispone de la base legal de conformidad con las disposiciones establecidas en la LFPDPPP y demás normativa aplicable para llevar a cabo el tratamiento de cualquier dato personal necesario para la recolección de dichas opiniones y sin perjuicio de que se adopten las medidas necesarias para la protección de los intereses de la organización.

Si la decisión final del responsable del tratamiento difiere de las opiniones de los titulares interesados, sería recomendable que este documente sus motivos para continuar con el mismo o no. En dado caso que el responsable decida no recabar la opinión de los titulares interesados, se recomienda documentar la justificación de su decisión, por ejemplo, toda vez que sea desproporcionado o impracticable o que atente contra los intereses de la organización.

Otra buena práctica en el proceso de elaboración de la EIP es la de definir y documentar otras funciones y responsabilidades específicas, tomando en consideración la política interna y procesos de la organización, tales como recabar el asesoramiento de expertos relacionados con la materia.

En resumen, los actores involucrados en la puesta en operación de una EIP podrán ser:

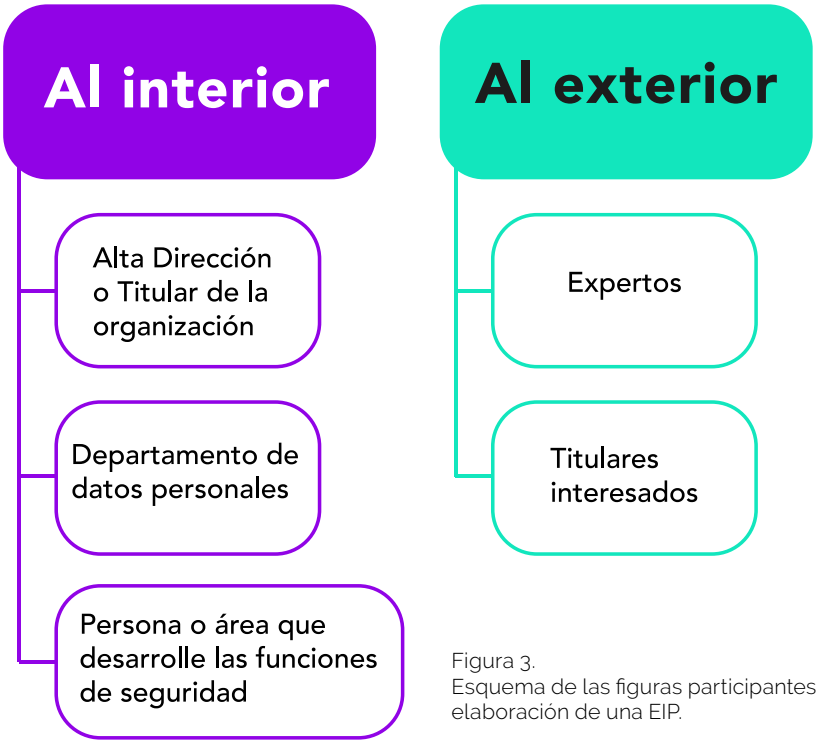

Figura 3.
Esquema de las figuras participantes en la elaboración de una EIP.

¿Cuál es la metodología para llevar a cabo una EIP?

No existe como tal una metodología única para realizar una EIP, por lo que, los responsables podrán elegirla de conformidad con las características del tratamiento a evaluar.

Como bien se ha señalado, la normativa aplicable al sector privado no prevé la figura y concepto de EIP, por lo que, en este apartado tal y como se señaló en el marco de referencia, cada responsable que decida realizar una EIP, como buena práctica, podrá hacer uso de referencias internacionales en la materia para llevar a cabo su EIP. También podrá identificar las herramientas de facilitación que el INAI, en ejercicio de su atribución contenida en el artículo 39, fracción III, de la LFPDPPP, ha elaborado para proporcionar apoyo técnico a los responsables para el cumplimiento de sus obligaciones, con la finalidad de identificar aquellas que resultan de utilidad para cada una de las etapas del procedimiento en caso de que proceda a realizar su EIP.

Como criterio orientador, de conformidad con lo previsto en las Directrices sobre la EIPD, el RGPD establece las características mínimas de una EIP (artículo 35, apartado 7, y considerandos 84 y 90):

> *- «una descripción [...] de las operaciones de tratamiento previstas y de los fines del tratamiento»;*
> *- «una evaluación de la necesidad y la proporcionalidad» del tratamiento;*
> *- «una evaluación de los riesgos para los derechos y libertades de los interesados»;*
> *- «las medidas previstas para: o afrontar los riesgos»; o «demostrar la conformidad con el presente Reglamento».*

A partir de lo anterior se identifica el siguiente procedimiento genérico en el que se señalan las etapas de una EIP:

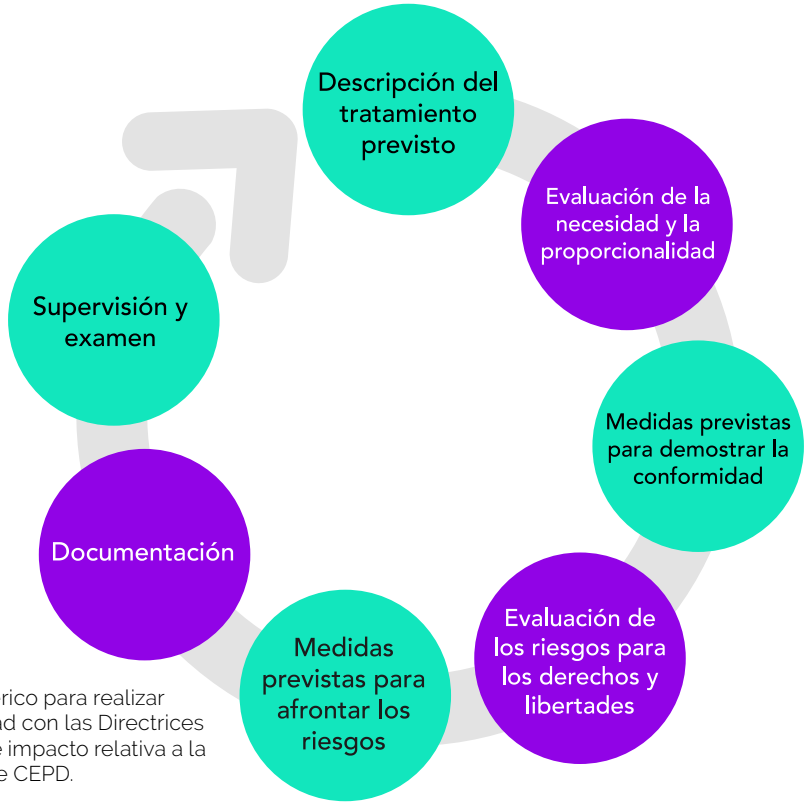

Figura 4.
Proceso iterativo genérico para realizar una EIP de conformidad con las Directrices sobre la evaluación de impacto relativa a la protección de datos de CEPD.

En este sentido, las Directrices EIPD mencionan que el RGPD ofrece un marco amplio y genérico para diseñar y llevar a cabo una EIP, los cuales pueden verse complementados con una orientación práctica más detallada. Precisando que lo dispuesto en el presente párrafo es únicamente con fines orientadores, puesto que no existe ninguna vinculación jurídica con la adopción o implementación del RGPD por parte de nuestro país y, por ende, su mención se realiza únicamente como un ejercicio de difusión de mejores prácticas identificadas.

Ahora bien, en el contexto mexicano la LFPDPPP no contempla un procedimiento específico para tal efecto, por lo que, serán los responsables quienes puedan diseñar

y aplicar una EIP que sea apta para sus operaciones de tratamiento, tomando siempre en cuenta los recursos disponibles en función de las características de su organización, por lo que, existe flexibilidad para los responsables del tratamiento para determinar la estructura y forma precisas de la EIP con el fin de permitir que esta se ajuste a las prácticas de trabajo ya existentes.

No obstante, como lo señala el CEPD, sin importar su forma, una EIP debe representar una auténtica evaluación de los riesgos que permita a los responsables tomar medidas para abordarlos.

En virtud de lo anterior, a continuación, se abordarán cada una de las etapas genéricas del procedimiento y se acompañará de la identificación de aquellas herramientas que resulten aplicables y que puedan facilitar a los responsables la realización de una EIP, las direcciones electrónicas de cada herramienta se encuentran contenidas en una tabla de referencia al final de la presente Guía.

Descripción del tratamiento previsto

¿Cuál es el objetivo de esta etapa?
Como inicio del proceso, se prevé que el responsable elabore una descripción sistemática de las operaciones de tratamiento previstas, de la naturaleza, del ámbito, del contexto y de los fines del tratamiento.

¿De qué puedo hacer uso?

I. Consultar la información disponible en las secciones II. *Conceptos básicos para entender esta guía y III. Diagnóstico inicial: lo primero que debo hacer para cumplir con mis obligaciones de la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.*

Evaluación de la necesidad y la proporcionalidad

¿Cuál es el objetivo de esta etapa?
Una vez descrito el tratamiento previsto, se deberá analizar la necesidad y proporcionalidad de las operaciones con respecto a su finalidad, por lo que es necesario tener claro qué datos se van a tratar y su finalidad, así como la licitud del tratamiento.

¿De qué puedo hacer uso?

Consultar las secciones correspondientes a los principios de licitud, finalidad y proporcionalidad de la *Guía LFPDPPP*.

Responder el "Listado de comprobación" correspondiente para cada uno de los principios señalados, mismo que se encuentra al final de cada sección.

Medidas previstas para demostrar la conformidad

¿Cuál es el objetivo de esta etapa?
El responsable deberá adoptar medidas para demostrar la conformidad con las disposiciones establecidas en el marco normativo que le resulte aplicable en materia de protección de datos personales.

¿De qué puedo hacer uso?

Responder los *"Listados de comprobación"* correspondiente para cada uno de los principios y deberes rectores de la protección de datos personales que se encuentran disponible en la *Guía LFPDPPP.*

Consultar la *Tabla de Equivalencia Funcional entre estándares de seguridad, la LFPDPPP, su Reglamento y las Recomendaciones en Materia de Protección de Datos Personales,* la cual es un material de referencia para que responsables y encargados del tratamiento de datos personales evalúen en su organización, el cumplimento de los requisitos y obligaciones que establece la LFPDPPP, su RLFPDPPP y las recomendaciones en materia de seguridad de los datos personales, a través de un esquema que correlaciona a la norma con los objetivos de control de los principales estándares internacionales en materia de seguridad de la información y privacidad.

Hacer uso de las herramientas para dar cumplimiento al principio de información tales como:

- Consultar la *Guía ABC del aviso de privacidad para el sector privado;*
- Verifique que su aviso de privacidad contenga los elementos informativos obligatorios registrando el *Formato de autoevaluación de aviso de privacidad sector privado;*
- Hacer uso del *Generador de Avisos de Privacidad para el sector privado.*
- Consultar la *Guía para Instrumentar Medidas Compensatorias*.
- Consultar la *Guía práctica para la atención de las solicitudes de ejercicio de los derechos ARCO*

Atender a lo previsto en las Recomendaciones para la Designación de la Persona o Departamento de Datos Personales.

Si es necesaria la selección y contratación de proveedores, para los servicios de infraestructura, plataforma y software del denominado cómputo en la nube, tomar en cuenta lo que disponen los *Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube* que impliquen el tratamiento de datos personales.

Para la cancelación de los datos personales consultar lo dispuesto por la *Guía para el borrado seguro de datos personales.*

Evaluación de los riesgos para los derechos y libertades

¿Cuál es el objetivo de esta etapa?
Todo responsable deberá realizar una evaluación de los riesgos (origen, la naturaleza, la particularidad y la gravedad) desde la perspectiva de los derechos y libertades de los titulares.

¿De qué puedo hacer uso?

Con relación a los riesgos para la seguridad de la información:

Hacer uso del *Evaluador de Vulneraciones* para registrar y documentar las medidas de seguridad existentes y faltantes, que ayuden a minimizar la ocurrencia y el impacto de vulneraciones a la seguridad de los datos personales, a través de una serie de preguntas cerradas, relacionadas con riesgos en el tratamiento de datos personales.

Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, la cual contiene los pasos claves para crear un Sistema de Gestión de Seguridad de Datos Personales basado en el ciclo Planear-Hacer-Verificar-Actuar (PHVA), de manera que a través de un proceso de mejora continua se logre un nivel aceptable del riesgo en el tratamiento de la información personal, de acuerdo con el modelo y objetivos de la organización.

Medidas previstas para afrontar los riesgos

¿Cuál es el objetivo de esta etapa?
Es importante que el responsable identifique las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales en cada una de las etapas del ciclo de vida de los datos.

¿De qué puedo hacer uso?

Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas, para la identificación e implementación de controles de seguridad adecuados para la protección de los datos personales.

Recomendaciones para el manejo de incidentes de seguridad de datos personales, en el cual se describen los procesos y controles recomendados por el Instituto para generar un plan de respuesta a incidentes de seguridad, en particular para mitigar las vulneraciones a la seguridad de los datos personales. Estas recomendaciones ayudarán y orientarán a los responsables para lo siguiente:

- Reconocer las diferencias entre alertas e incidentes de seguridad.
- Elaborar un plan para responder ante incidentes de seguridad, conforme estándares internacionales.
- Utilizar formatos de referencia para documentar los incidentes de seguridad.

Metodología de análisis de riesgo BAA, la cual analiza el riesgo de los datos personales en función de tres factores: (i) el beneficio para el atacante, (ii) la accesibilidad de la información, y (iii) la posible anonimidad del atacante.

Manual en materia de seguridad basada en un entorno Microsoft® para MIPYMES y organizaciones pequeñas mexicanas.

Documentación

¿Cuál es el objetivo de esta etapa?
Todo responsable que implemente una EIP podrá documentar cada una de las etapas del proceso con la finalidad de generar evidencia con relación al cumplimiento de las obligaciones en materia de protección de datos personales. Por lo anterior, resultará de suma importancia mantener evidencia de todas y cada una de las acciones realizadas, puesto que estas sustentarán las conclusiones y medidas de seguridad físicas, técnicas y administrativas que se determinen para desarrollar un adecuado tratamiento de datos personales..

¿De qué puedo hacer uso?

Sistemas tecnológicos generados al interior de la organización en los que se acredite la documentación de cada una de las acciones.

Llenado de formatos generados por el responsable para acreditar las acciones realizadas en cada etapa.

Publicación de los resultados de la información a través del medio de comunicación que considere pertinente.

Supervisión y examen

¿Cuál es el objetivo de esta etapa?
Como etapa final de proceso se prevé que el responsable establezca los mecanismos para que se realice una evaluación de los resultados de la EIP con la finalidad de que se identifiquen las acciones a seguir y en su caso estas sean supervisadas por parte del área correspondiente dentro de su organización interna.

¿De qué puedo hacer uso?
Se sugiere al finalizar, una vez que se hayan identificado los posibles riesgos que conlleve el tratamiento de datos personales que se pretende implementar, se determine si será necesario consultar al INAI para efectos de recibir apoyo técnico y las recomendaciones respectivas. De manera adicional a lo descrito en el presente apartado, se incluyen un listado de documentos que contienen distintas metodologías desarrolladas por otras autoridades de protección de datos personales en función principalmente del RGPD, mismas que podrán servir de referencia para que cada responsable identifique sus necesidades y realice su EIP. Los documentos señalados podrán ser consultados en la sección de Fuentes de referencia de esta Guía.

¿Existe la obligación de publicar la EIP?

No, pero publicar un resumen podría fomentar la confianza con los titulares respecto al cumplimiento de los principios, deberes y derechos de estos últimos.

La publicación de una versión resumida de la EIP no representa un requisito jurídico, sin embargo, podría suponer una práctica particularmente positiva, ya que es una decisión que corresponde al responsable del tratamiento. Sin embargo, como buena práctica, los responsables podrían considerar al menos la publicación de algunas partes, como un resumen o una conclusión de su EIP toda vez que la información contenida en el documento completo puede dar cuenta de medidas de seguridad y procesos o procedimientos confidenciales o sensibles del responsable o sobre proyectos comerciales que representan ventajas o desventajas respecto de otros.

En este sentido, la EIP publicada no necesita contener toda la evaluación, se sugiere que la versión publicada podría consistir en un resumen de las principales conclusiones de la EIP o incluso únicamente en una declaración que afirmarse que esta se ha llevado a cabo.

Lo anterior con la finalidad de fomentar la expectativa razonable de privacidad, prevista en el artículo 7 de la LFPDPPP, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por la LFPDPPP.

De manera adicional, la difusión de los resultados de la EIP permitiría al responsable ayudarle con el cumplimiento del principio de responsabilidad, previsto en los artículos 6 y 14 de la LFPDPPP, consistente en la obligación de los responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y la autoridad, que cumple con sus obligaciones en torno a la protección de los datos personales.

Finalmente, cuando el resultado de una EIP revele unos elevados riesgos residuales, se sugiere al responsable del tratamiento realizar una consulta ante el INAI en términos de lo previsto en el artículo 39, fracción III, de la LFPDPPP, previo a que se realice el tratamiento, motivo por el cual, se debe facilitar toda la información relativa a la realización de la EIP.

¿Puedo consultar al INAI?

En primer lugar, es de mencionar que, de conformidad con lo dispuesto en el artículo 39, fracciones III y IV , de la LFPDPPP, el Instituto tiene las atribuciones para proporcionar apoyo técnico a los responsables que así lo soliciten, así como la de emitir recomendaciones de conformidad con las disposiciones aplicables de dicha ley para efectos de su funcionamiento y operación.

En específico, el artículo 42, fracción II del Estatuto Orgánico del INAI establece que entre las funciones de la Dirección General de Normatividad y Consulta se encuentra atender consultas en materia de protección de datos personales de los sectores público y privado.

En este sentido, todo responsable podrá acudir al INAI en cualquier momento para solicitar la asesoría y consulta en la materia, incluso derivado de la toma de decisión de realizar una EIP como buena práctica, previo a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes. Por lo tanto, se podrá acudir al INAI para que, en ejercicio de las atribuciones señaladas, emita la opinión técnica respectiva o proporcione el asesoramiento y apoyo necesario cuando:

1. Después de haber realizado como buena práctica una EIP, el responsable identifique riesgos que incidan sobre elementos normativos cuya aplicación o interpretación no sea clara, y se encuentre dentro del ámbito de atribuciones del INAI su interpretación.
2. Se identifiquen elementos relacionados con transferencias nacionales o internacionales de datos personales, así como cualquier otro tratamiento relacionado con flujos transfronterizos de datos personales, en los cuáles existan conflictos o dudas en torno a la jurisdicción o aplicabilidad de disposiciones generales o específicas, tomando en consideración a los actores que se encuentren involucrados en dicho tratamiento.
3. En cualquier otro supuesto en el que se identifique que resulte necesario el apoyo técnico en el ámbito de atribuciones del INAI, incluyendo, el análisis de los controles implementados a partir de los riesgos detectados en la elaboración de la EIP y los criterios de cumplimiento de la LFPDPPP.

Supuestos sobre los cuáles se elaboraría la opinión o brindaría el asesoramiento de referencia, conforme a los plazos y procedimientos aplicables para la atención de consultas.

Resulta importante señalar que el INAI constituye un sujeto obligado en materia de transparencia y acceso a la información pública, por lo que, toda la información bajo su posesión es susceptible de considerarse información pública.

Por tanto, considerando que las EIP pueden contener información de carácter clasificado como confidencial, resultaría deseable que la solicitud de consulta que se presente ante el INAI precise qué información de la que acompaña a la consulta se considera clasificada como confidencial y que, en su caso, se solicite su devolución conjuntamente con la respuesta, resultando deseable, se señalen las personas autorizadas para recibir dicha información a través de la misma solicitud.

Como la elaboración de las opiniones técnicas se elaboran directamente por parte del INAI, es decir, sin que medien formalidades de un procedimiento, solamente podrán quedar comprendidas dentro de dichas opiniones aquellos aspectos que se

desprendan de los elementos proporcionados, en el entendido que, ante la falta de condiciones para poder emitir una opinión, bastará con que se señale dicha circunstancia, sin perjuicio de que el responsable se encuentre en aptitud de volver a solicitar una nueva opinión técnica.

Aunado a ello, se recomienda a los responsables tomar las medidas de seguridad correspondientes para la presentación de la información ante el INAI, ya que a esta institución le corresponde su protección a partir de su recepción por la Oficialía de Partes, por ello, cualquier actividad o diligencia previa no puede quedar comprendida. Asimismo, el responsable podrá conocer las condiciones sobre las cuales se llevará a cabo el tratamiento de los datos personales al acceder al apartado de avisos de privacidad puestos a disposición del INAI para su consulta.

Finalmente, dadas las características del marco normativo de la LFPDPPP, conviene señalar que la opinión técnica que emita el INAI con motivo del asesoramiento brindado no es vinculante, por lo cual, no tiene por efecto impedir la puesta en operación o modificación, ni validar el presunto cumplimiento de las obligaciones a cargo de los responsables. En consecuencia, si derivado de la opinión que en su caso emita el INAI, se desprendiera el incumplimiento potencial de alguna disposición de la LFPDPPP por parte del responsable, o algún riesgo elevado inherente a los resultados identificados con la EIP, corresponde valorar al responsable la operación o modificación del tratamiento que corresponda, sin responsabilidad, postura o posición por parte del INAI.

Preguntas frecuentes

¿El procedimiento para realizar la EIP del sector privado se encuentra previsto en alguna normativa?

No, el marco normativo en materia de protección de datos personales respecto a este sector no establece la figura de EIP, sin embargo, como fue señalado, el presente documento establece un marco de referencia de la metodología y las etapas del procedimiento para realizar una EIP de conformidad con las Directrices EIPD, reiterando que será el responsable quien determine el procedimiento que considere adecuado en función de las características de su organización.

¿Se sugiere utilizar el procedimiento para evaluaciones de impacto en la protección de datos personales previsto por la LGPDPPSO para realizar una EIP?

No. Como bien se dijo en la presente guía, el responsable puede hacer uso de cualquier metodología, sin embargo, se observa que las evaluaciones de impacto en la protección de datos personales previstas por la LGPDPPSO se dirigen especialmente a sujetos obligados, conforme a un procedimiento establecido de manera específica para su tramitación, por lo cual, ante la falta de referencia de cualquier otra metodología o proceso, se sugiere utilizar directamente los elementos proporcionados en la presente guía, los cuales están pensados para su aplicación en el marco de la de la protección de datos personales en posesión de los particulares.

¿A través de qué medio puedo consultar al INAI?

Las consultas podrán presentarse a través de los siguientes medios:

- Por escrito en las oficinas del INAI;
- A través del Centro de Atención a la Sociedad, que se encuentra ubicado en Avenida Insurgentes Sur número 3211, Colonia Insurgentes Cuicuilco, Alcaldía Coyoacán, Código Postal 04530, Ciudad de México, México o por medio de su correo electrónico atencion@inai.org.mx.
- Directamente al correo electrónico: normatividadyconsulta@inai.org.mx.

EIP con resultado de riesgo elevado ¿Puedo realizar el tratamiento?

En aquellos casos en los que se lleve a cabo como buena práctica la EIP y se concluya con un riesgo elevado, se sugiere que el responsable del tratamiento realice una consulta al INAI para que, en ejercicio de sus atribuciones de apoyo técnico y de emisión de criterios y recomendaciones, previstas en el artículo 39, fracciones III y IV reciba apoyo técnico, y orientación para determinar si es posible realizar la nueva modalidad de tratamiento y/o la realización de la modificación sustancial en tratamientos ya existentes, reiterando que la decisión final, corresponderá únicamente al responsable del tratamiento, tal como se refiere en la presente guía.

Si ya realicé una EIP, ¿es necesario actualizarla?

La EIP es un proceso que no se agota una vez realizado, sino que implica un proceso de continua inspección, por lo que, es necesario que exista una revisión y monitoreo periódico para identificar si se han producido cambios en los riesgos que el tratamiento implica con relación al momento en que el tratamiento se puso en marcha. Por lo que, siempre que existan modificaciones sustanciales en el tratamiento que pueda suponer un incremento en el nivel de riesgo asociado al mismo, será necesario realizar una actualización de la EIP ya realizada o en su caso, considerando, nuevas tecnologías, cambio de finalidad, tratamiento de datos distintos o en diferente cantidad, efectuar una nueva evaluación.

Fuentes de referencia

1. Agencia Española de Protección de Datos, Guía práctica para LAS Evaluaciones de Impacto en la Protección de LOS datos sujetas al RGPD, https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf
2. Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", 01037/12/EN, WP 196, July 2012 (Web reference: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
3. Cayirci E., Garaga A., De Oliveira A.S., Roudier Y., "Cloud Adoption Risk Assessment Model", IEEE Proceedings of Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on, pp. 908-913, December 2014, DOI:

10.1109/UCC.2014.148 (Web Reference: http://www.eurecom.fr/fr/publication/4465/detail/a-cloud-adoption-risk-assessment-model)

4. Commission nationale de l'informatique et des libertés (CNIL), PIA Guides, https://www.cnil.fr/fr/node/24129
5. DoD Privacy Impact Assessment (PIA) Guidance, http://www.dtic.mil/whs/directives/corres/pdf/540016p.pdf
6. European Union Agency for Cybersecurity (ENISA), Cloud Computing Risk Assessment, November 20, 2009, https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
7. Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada, http://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_201103/
8. Finn R., Wright D., Friedewald M., Seven types of privacy. In: European Data Protection: Coming of Age? (Gutwirth S., Leenes R., De Hert P., et al., eds.). Springer, Dordrecht, 2013
9. Grupo "Protección de Datos" del Artículo 29, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
10. HIMSS Privacy Impact Assessment Guide, http://www.himss.org/sites/himssorg/files/HIMSSorg/Content/files/D87_HIMSS_PIA_Guide_.pdf
11. Information Commissioner's Office (ICO), "Conducting privacy impact assessments code of practice", February 2014, https://www.pdpjournals.com/docs/88317.pdf
12. ISO 14300-1:2011, Space systems — Programme management — Part 1: Structuring of a project
13. ISO 21500, Guidance on project management
14. ISO 22307, Financial services — Privacy impact assessment
15. ISO 27005, Information technology — Security techniques — Information security risk management
16. ISO 31000, Risk management — Principles and guidelines
17. ISO 722, Rock drilling equipment — Hollow drill steels in bar form, hexagonal and round

18. ISO 9000:2015, Quality management systems — Fundamentals and vocabulary
19. ISO/IEC 16509:1999, Information technology — Year 2000 terminology
20. ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements
21. ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls
22. ISO/IEC 29134:2017, Information technology — Security techniques — Guidelines for privacy impact assessment
23. ISO/IEC 29151:2017, Information technology — Security techniques — Code of practice for personally identifiable information protection
24. NIST/SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
25. NIST/Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Recommendations of the National Institute of Standards and Technology
26. PIA Framework for RFID Applications, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf
27. PIA Guidelines German BSI
28. PIA Manual, CNIL, 2015, http://www.cnil.fr/english/news-and-events/news/article/privacy-impact-assessments-the-cnil-publishes-its-pia-manual/
29. Privacy Impact Assessments: International Study of their Application and Effects October, 2007 Linden Consulting, Inc.
30. Public Law 107–347—DEC. 17 2002, https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf
31. Report E.N.I.S.A. "Cloud Computing Risk Assessment - Benefits, risks and recommendations for information security", November 2009 (Web reference:
32. https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment)
33. Tancock | Pearson | Charlesworth: The Emergence of Privacy Impact Assessments, http://www.hpl.hp.com/techreports/2010/HPL-2010-63.pdf
34. The ICO PIA Handbook
35. The Privacy Office Official Guidance – June 2010, US Department of Homeland

Security – Privacy Office, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf

36. Treasury Board of Canada Secretariat Directive on Privacy Impact Assessments, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308
37. Trilateral Research & Consulting, "Privacy impact assessment and risk management Report for the Information Commissioner's Office prepared by Trilateral Research & Consulting", 4 May 2013, https://ico.org.uk/media/1042196/trilateral-full-report.pdf
38. Trilateral Research & Consulting, "Privacy Impact Assessment executive summary",https://ico.org.uk/media/1042837/trilateral-report-executive-summary.pdf
39. Wright D., de Hert P., eds. Privacy Impact Assessment. Springer, Dordrecht, 2012
40. Wright D., Making privacy impact assessment more effective. Inf. Soc. 2013, 29 (5) pp. 307–315. Available at: http://www.indiana.edu/~tisj/29/index.html#5
41. Wright D., The state of the art in privacy impact assessment. Comput. Law Secur. Rev. 2012 Feb., 28 (1) pp. 54–61. Available at: http://www.sciencedirect.com/science/journal/02673649

Herramientas de facilitación elaboradas por el INAI que podrán ser utilizadas para la EIP

Nombre de la herramienta	Dirección electrónica
Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales	http://inicio.inai.org.mx/nuevo/ComputoEnLaNube.pdf
El ABC del Aviso de Privacidad	http://abcavisosprivacidad.ifai.org.mx/
Evaluador de Vulneraciones	http://inicio.ifai.org.mx/SitePages/Evaluador-Vulneraciones.aspx
Formato de Autoevaluación de Aviso de Privacidad Sector Privado	http://inicio.inai.org.mx/AvisoPrivacidad/Autoevaluaci%C3%B3n%20responsable%20sector%20privado%2016mar17.docx

Generador de Avisos de Privacidad para el sector privado	https://generador-avisos-privacidad.inai.org.mx/users/login
Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares	http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf
Guía para el borrado seguro de datos personales	http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf
Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales	http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf
Guía para Instrumentar Medidas Compensatorias	http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_para_instrumentar_medidas_compensatorias.pdf
Guía práctica para la atención de las solicitudes de ejercicio de los derechos ARCO	http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf
Manual en materia de seguridad basada en un entorno Microsoft® para MIPYMES y organizaciones pequeñas mexicanas	http://inicio.ifai.org.mx/DocumentosdeInteres/Manual_Microsoft.pdf
Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas	http://inicio.ifai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf
Metodología de análisis de riesgo BAA	http://inicio.ifai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf
Recomendaciones para el manejo de incidentes de seguridad de datos personales	http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

Recomendaciones para la Designación de la Persona o Departamento de Datos Personales	http://inicio.ifai.org.mx/DocumentosdeInteres/RecomendacionesDesignar.pdf
Tabla de Equivalencia Funcional entre estándares de seguridad, la LFPDPPP, su Reglamento y las Recomendaciones en Materia de Protección de Datos Personales	http://inicio.ifai.org.mx/DocumentosdeInteres/Tabla_de_Equivalencia_Funcional(Junio2015).pdf

Legislación consultada

Nacional

Ordenamiento	Fecha de publicación en el DOF	Última reforma en el DOF	Vínculo electrónico
Constitución Política de los Estados Unidos Mexicanos	05-02-1917	08-05-2020	http://www.diputados.gob.mx/LeyesBiblio/pdf/1_080520.pdf
Ley Federal de Protección de Datos Personales en Posesión de los Particulares	05-07-2010	05-07-2010	http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	26-01-2017	26-01-2017	http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf
Reglamento de la Ley Federal de Protección de datos Personales en Posesión de los Particulares	21-12-2011	21-12-2011	http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf
Lineamientos del Aviso de privacidad	17-01-2013	17-01-2013	http://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013

Legislación consultada

Internacional

Ordenamiento	Vínculo electrónico
Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, Francia	https://www.oas.org/es/sla/ddi/docs/U12%20convenio%20n%20108.pdf https://www.dof.gob.mx/nota_detalle.php?codigo=5526265&fecha=12/06/2018
Estándares de Protección de Datos Personales para los Estados Iberoamericanos	https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf
REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE	https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&-from=ES

• Insurgentes Sur 3211, Col. Insurgentes Cuicuilco, Alcaldía Coyoacán, C.P. 04530

• Teléfono: 5004 2400 • www.inai.org.mx