Guía para la elaboración, presentación y valoración de

# Evaluaciones de Impacto

en la Protección de Datos Personales

REGIÓN
CENTRO
OCCIDENTE

SISTEMA NACIONAL
DE TRANSPARENCIA
ACCESO A LA INFORMACIÓN PÚBLICA
Y PROTECCIÓN DE DATOS PERSONALES

# Directorio

Instituto de Transparencia del Estado de Aguascalientes

Jorge Armando García Betancourt
Comisionado Presidente

Mónica Janeth Jiménez Rodríguez
Comisionada

Óscar González Manríquez
Comisionado

Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos del Estado de Colima

Francisco José Yáñez Centeno y Arvizu
Comisionado Presidente
Ayizde Anguiano Polanco
Comisionada
Paulina Alejandra Urzúa Gómez
Comisionada

Instituto de Acceso a la Información Pública para el Estado de Guanajuato

Mariela del Carmen Huerta Guerrero
Comisionada Presidenta
Juan Sámano Gómez
Comisionado
Francisco Antonio Alejandro Rocha Pedraza
Comisionado

Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco

Olga Navarro Benavides
Comisionada Presidenta
Salvador Romero Espinosa
Comisionado
Pedro Antonio Rosas Hernández
Comisionado

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

Abraham Montes Magaña
Comisionado Presidente
Ruth Nohemí Espinoza Pérez
Comisionada
Areli Yamilet Navarrete Naranjo
Comisionada

Instituto de Transparencia y Acceso a la Información Pública del Estado de Nayarit

Ramón Alejandro Martínez Álvarez
Comisionado Presidente
Esmeralda Isabel Ibarra Beas
Comisionada
Alejandra Langarica Ruiz
Comisionada

Comisión de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Querétaro

Javier Marra Olea
Comisionado Presidente
Alejandra Vargas Vázquez
Comisionada
Octavio Pastor Nieto de la Torre
Comisionado

Comisión Estatal de Garantía de Acceso a la Información Pública del Estado de San Luis Potosí

David Enrique Menchaca Zúñiga
Comisionado Presidente
Ana Cristina García Nales
Comisionada
José Alfredo Solís Ramírez
Comisionado

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

Fabiola Gilda Torres Rodríguez
Comisionada Presidenta
Nubia Coré Barrios Escamilla
Comisionada
Samuel Montoya Álvarez
Comisionado

Edición, mayo de 2024.

# Contenido

# 1. Presentación.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el día 26 de enero de 2017, sentó las bases para el tratamiento de los datos personales en posesión de sujetos obligados, el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos, así como el derecho a la portabilidad.

Dicha ley reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, también trajo consigo un nuevo catálogo de *"Acciones Preventivas en Materia de Protección de Datos Personales"*, entre las que se contempla la denominada *"Evaluación de Impacto en la Protección de Datos Personales"*.

Esta acción preventiva, constituye una obligación a cargo de los responsables que pretendan realizar un tratamiento intensivo o relevante de datos personales, derivado de la puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología.

Con esta Guía, se da cara a los retos que implican el uso de nuevas tecnologías, permitiendo a los responsables prevenir el uso indebido de datos personales o la probable vulneración a la que se encuentran expuestos dentro del entorno digital.

Para tal efecto, a fin de brindar certeza en la elaboración, presentación, y valoración de las evaluaciones de impacto, el Sistema Nacional de

Transparencia, Acceso a la Información Pública y Protección de Datos Personales, emitió la norma técnica a través de las Disposiciones Administrativas de carácter general que regulan dicha materia. Esta norma fue publicada en el Diario Oficial de la Federación el 23 de enero de 2018, normativa que desarrolla puntualmente los pasos para llevar a cabo una evaluación de impacto.

En ese orden de ideas, con el objetivo de contar con un instrumento que facilite el entendimiento de las etapas que implican una Evaluación de Impacto en la Protección de Datos Personales, desde su elaboración hasta su valoración y, en su caso, emisión del respectivo dictamen, se crea el presente documento, que pretende servir como insumo y apoyo para los Organismos Garantes Locales en la tramitación de estos procesos.

Por lo expuesto, en aras de garantizar el derecho humano a la protección de datos personales, se emite la presente Guía.

# 2. Consideraciones preliminares.

## 2.1. Glosario.

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

**Datos personales sensibles.** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. Entre estos, pueden mencionarse a manera de ejemplo: 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, preferencia sexual, entre otros.

**Datos biométricos.** Datos personales de carácter sensibles referentes a las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, mesurables y que conciernen a una persona física identificada o identificable.

**Datos personales biométricos.** Son aquellos rasgos físicos, biológicos o de comportamiento de un individuo que lo identifican como único del resto de la población; huellas dactilares, geometría de mano, análisis de iris, análisis de retina, venas del dorso de la mano, rasgos faciales, patrón de voz, firma manuscrita, dinámica de tecleo, cadencia del paso al caminar, análisis gestual y análisis de ADN.

**Medidas de seguridad administrativas.** Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales a nivel

organizacional, la identificación, clasificación y borrado seguro de los datos personales, así como la sensibilización y capacitación del personal en materia de protección de datos personales.

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

**Medidas de seguridad técnicas.** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

**Oficial de Protección de Datos.** Persona servidora pública especializada en la materia, que forma parte de la Unidad de Transparencia, encargada de realizar las atribuciones que, en materia de protección de datos personales, corresponden a la citada unidad.

**Responsable.** Los sujetos obligados que deciden sobre el tratamiento de datos personales.

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

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

**Tratamiento.** Cualquier tipo de acción u operación que implique la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

## 2.2. Legislación.

I. Constitución Política de los Estados Unidos Mexicanos.

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

III. Leyes locales de Protección de Datos Personales en Posesión de Sujetos Obligados.

IV. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

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

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

## 2.3. Abreviaturas.

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

**EIPD.** Evaluación de Impacto en la Protección de Datos Personales.

**OGL.** Organismo Garante Local.

**Proyecto.** Política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales que el Sujeto Obligado pretende operar o modificar.

**LGPDP.** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

**LPDPL.** Ley de Protección de Datos Personales Locales.

## 2.4. ¿Qué es una Evaluación de Impacto de Protección en la Datos Personales?

De conformidad con la LGPDP y las LPDPL, la Evaluación de Impacto de Protección de Datos Personales es el documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el ***tratamiento intensivo o relevante*** de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

A través de dicho documento de análisis, se realiza una valoración en cuanto al impacto que tendrá un tratamiento intensivo o relevante de datos personales, identificando los factores de riesgo existentes y estableciendo las medidas administrativas, físicas y técnicas para mitigarlos.

En suma, la EIPD se define como una herramienta con carácter preventivo que deben realizar los sujetos obligados para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas.

## 2.5. Importancia de la EIPD.

La evaluación de impacto como medida preliminar a la implementación de un proyecto que implica el tratamiento intensivo de datos personales es una herramienta de gran valor y utilidad, pues pone sobre advertencia los probables riesgos que la ejecución del proyecto podría conllevar, permitiendo al responsable prever las medidas de seguridad necesarias para mitigar estos, observando con ello los deberes y principios previstos por la ley general en la materia, así como por las legislaciones locales.

Otro aspecto relevante de las EIPD es la metodología que los responsables deben llevar a cabo para su realización, toda vez que involucra un análisis normativo y

tecnológico, detallando los datos personales sujetos a tratamiento, las categorías de titulares, las finalidades del tratamiento, la tecnología a implementar y sus medidas de seguridad, entre otros aspectos, que permiten al sujeto obligado conocer a profundidad los alcances e implicaciones que el desarrollo del proyecto conlleva.

En ese sentido, la EIPD es una herramienta de gran utilidad, pues facilita a los responsables identificar los probables riesgos que la puesta en operación de un proyecto involucra, permitiendo establecer medidas para su mitigación, así como permite a los OGL garantizar en mayor medida el respeto y observancia de las disposiciones legales en la materia.

## 2.6. ¿Qué es un tratamiento intensivo o relevante de datos personales?

Se entiende por tratamiento intensivo o relevante a aquel que es aplicado en tal magnitud o importancia en el que se identifique un riesgo potencial que pudiera representar un agrave afectación a la protección de los datos del titular.

El artículo 75 de la LGPDP contempla tres supuestos para considerar cuándo se está en presencia de un tratamiento intensivo o relevante de datos personales, siendo estos:

a. Existan riesgos inherentes a los datos personales a tratar.

b. Se traten datos personales sensibles.

c. Se efectúen o pretendan efectuar transferencias de datos personales.

Por su parte, las Disposiciones Administrativas, establecen dos criterios para determinar cuándo un tratamiento de datos personales tiene carácter intensivo o relevante, para lo cual, lo divide en:

a. Tratamiento intensivo de datos personales de carácter general.

b. Tratamiento Intensivo de datos personales de carácter particular.

Bajo estos criterios, se entiende que se está ante un *tratamiento intensivo de datos personales de carácter general* cuando concurran algunas de las siguientes condiciones:

1. Los datos personales tengan un alto riesgo porque podrían ser valiosos para alguien que no debería tener acceso a ellos. Esto puede depender de qué tan sensibles sean los datos, cuántas personas estén involucradas, cuántos datos se manejen, con qué frecuencia se usan, y si se combinan con datos de otros sistemas o plataformas.

2. Se manejen datos personales privados y sensibles, como información sobre raza, salud, genética, creencias religiosas o políticas, y preferencias sexuales.

3. Se envíen datos personales a otros lugares o personas, dentro o fuera de México, especialmente si se hace regularmente y los datos son sensibles o se mandan a lugares con menos protecciones de privacidad.

Por otra parte, se estará ante un *tratamiento intensivo de datos personales de carácter particular* cuando el responsable pretenda:

1. Cambiar el propósito original de los datos para algo más invasivo de la privacidad.

2. Analizar o predecir comportamientos o características personales de manera detallada, lo que podría resultar en decisiones importantes que afecten legal o significativamente a las personas.

3. Manejar datos de personas en situaciones vulnerables considerando factores como edad, género, raza, salud, y nivel socioeconómico.

4. Crear grandes bases de datos, aunque inicialmente no se tenga un plan específico para su uso.

**5.** Añadir nuevos tipos de datos personales a bases ya existentes, lo que podría aumentar el riesgo si hay una vulneración de datos.

**6.** Manejar frecuentemente grandes cantidades de datos personales, o combinar información entre varios sistemas o plataformas tecnológicas.

**7.** Usar tecnologías avanzadas que involucren un manejo masivo de datos personales, como minería de datos, biometría, y geolocalización.

**8.** Dar acceso a terceros a muchos datos personales que antes no tenían, ya sea compartiéndolos o permitiendo su uso de alguna forma.

**9.** Enviar datos personales a países que no tienen leyes sólidas de protección de datos.

**10.** Utilizar nuevamente datos que se habían desvinculado o disociado de personas específicas.

**11.** Hacer un manejo extenso y sistemático de datos sensibles.

**12.** Evaluar de manera detallada y automática características personales para crear perfiles, y tomar decisiones basadas en estos, que tengan consecuencias legales importantes o impactos significativos similares en las personas.

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

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

## 2.7. ¿Cuándo se debe realizar una EIPD?

Cuando cualquiera de los Sujetos Obligados pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología y, a su juicio, considerando, lo dispuesto en las leyes aplicables, así como en las Disposiciones Administrativas, impliquen un tratamiento intensivo o relevante de datos personales.

Asimismo, al ser la EIPD un mecanismo preventivo, esta debe realizarse previo a la operación o modificación del proyecto a implementar, contemplando las Disposiciones Administrativas un plazo de al menos treinta días anteriores a su ejecución.

## 2.8. ¿Quién debe realizar una EIPD?

Cualquier dependencia, entidad, unidad de apoyo, órgano u organismo de los Poderes Ejecutivo, Legislativo y Judicial, organismos autónomos, partidos políticos, fideicomisos y fondos públicos, de los tres ámbitos de gobierno, que pretendan poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología y que esto implique un tratamiento intensivo o relevante de datos personales.

## 2.9. ¿Se puede eximir la presentación de una EIPD?

La LGPDP y las Disposiciones administrativas prevén dos supuestos de exención a la presentación de la EIPD, a saber:

a) Cuando a juicio del responsable se comprometan los efectos que se pretenden lograr con la posible puesta en operación o modificación del proyecto; y

b) Cuando a juicio del responsable se trate de situaciones de emergencia o urgencia.

En caso de que el responsable considere que se encuentra en alguno de los supuestos de exención, debe remitir al OGL un informe, durante los primeros treinta días hábiles posteriores a la fecha de la puesta en operación o modificación del proyecto, en el que exprese de manera fundada y motivada lo siguiente:

1. Denominación y objetivos generales y específicos del proyecto;
2. Finalidades del tratamiento intensivo o relevante de datos personales;
3. Razones y motivos por las cuales presentar la evaluación de impacto compromete los efectos del proyecto;
4. Descripción de la situación de emergencia o urgencia que hacen inviable la presentación de la evaluación de impacto;
5. Las consecuencias negativas que se derivarían de la elaboración y presentación de la evaluación de impacto;
6. El fundamento legal que habilitó el tratamiento en el marco del proyecto;
7. La fecha en que se puso en operación o modificó el proyecto y su periodo de duración;
8. La opinión técnica del oficial de protección de datos personales, en su caso, y
9. Los mecanismos o procedimientos adoptados por el responsable para que el proyecto cumpla, desde el diseño y por defecto, con todas las obligaciones previstas en la LGPDP, la LPDPL y demás disposiciones aplicables.

# 3. Metodología para llevar a cabo una EIPD.

## 3.1. Acciones previas a realizar una evaluación de impacto. Consultas.

**a) Consultas ante el OGL.** En caso de existir duda respecto de la elaboración y presentación de una EIPD, los responsables pueden realizar una consulta ante el OGL, con el objeto de establecer si es procedente su trámite, para lo cual deberán brindar a este los elementos que le permitan emitir una opinión técnica en la que determine si, conforme a la legislación aplicable, se actualiza o no la obligación del responsable de llevar a cabo la EIPD.

Para efectuar la consulta, el responsable deberá cubrir los requisitos previstos por el artículo 12 de las Disposiciones Administrativas. Asimismo, es pertinente señalar que, la consulta y la opinión técnica que de ella derive, no sustituyen a la obligación de elaborar y presentar la EIPD, pues su naturaleza es estrictamente aclaratoria.

**b) Consulta externa.** El responsable puede 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.

Dichas consultas deberán ser debidamente documentadas, permitiendo constatar su realización y la respuesta del público involucrado.

## 3.2. Evaluaciones de impacto interinstitucionales.

Existe la posibilidad de que, en virtud del ámbito de competencias, dos o más responsables sean los encargados de implementar o modificar un mismo proyecto, para lo cual, las Disposiciones Administrativas, prevén la posibilidad de que la pluralidad de responsables presente ante el OGL, de manera conjunta, una sola evaluación de impacto.

Para lo anterior, los responsables deberán presentar la EIPD conforme a las siguientes reglas:

a) Si los responsables son del orden federal, la presentación de ésta se deberá hacer ante el INAI;

b) Si los responsables son del orden federal, estatal y/o municipal, la presentación de esta se deberá hacer ante el INAI y los OGL competentes;

c) Si los responsables son del orden estatal y/o municipal de una sola entidad federativa, la presentación de ésta se deberá hacer ante el OGL de dicha entidad;

d) 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 OGL de dichas entidades federativas según corresponda, y

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

A las evaluaciones de impacto que sean presentadas de manera interinstitucional, les serán aplicables las disposiciones previstas para las EIPD presentadas por un solo responsable, en lo que refiere a generalidades, contenido y procedimiento de valoración, con las particularidades que específicamente se señalen.

## 3.3. Aspectos mínimos que debe contener la EIPD.

En toda EIPD, el OGL deberá verificar que el responsable señale, al menos, la siguiente información:

**a. 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.**

Dentro de la cuál, el responsable deberá indicar de forma precisa los siguientes elementos:

- Denominación del responsable del tratamiento de los datos personales (dependencia, entidad, unidad de apoyo, órgano, organismo, etc.).

- Denominación del proyecto (el nombre con el que se identifica a la política pública, programa, sistema, plataforma, etc.).

- Objetivos generales y específicos que persigue el proyecto.

- El fundamento legal del proyecto, conforme a las facultades o atribuciones que la normativa aplicable le confiere al responsable.

- Las categorías de los titulares, distinguiendo aquellos que pertenezcan a grupos vulnerables.

- Los datos personales que serán objeto de tratamiento, distinguiendo, en caso de existir, los que sean de carácter sensible.

- Las finalidades del tratamiento intensivo o relevante.

- Los procesos, fases o actividades operativas del proyecto, con una descripción puntual de los mismos.

- La forma en que se recabarán los datos personales o las fuentes de las cuales provienen.

- Las transferencias que, en su caso, se pretendan efectuar, señalando los destinatarios y su calidad (personas físicas o morales de carácter público o privado), así como los datos a transferir y su finalidad.

- El tiempo de duración del proyecto.

- La tecnología que se pretende utilizar.

- Las medidas de seguridad administrativas, físicas y técnicas a implementarse, de conformidad con la normativa aplicable.

- Nombre y cargo de los servidores públicos, con facultad expresa, para decidir, aprobar o autorizar la puesta en operación o modificación del proyecto.

- Cualquier otra información o documentos que considere conveniente hacer del conocimiento del OGL.

**b. 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.**

En dicha justificación el responsable debe señalar la siguiente información:

- Las razones o motivos que justifican la necesidad de iniciar o cambiar el proyecto, de acuerdo con sus objetivos generales y específicos.

- Si las medidas sugeridas son adecuadas para proteger los datos personales.

- Si estas medidas son las mínimas necesarias, es decir, las más moderadas para asegurar la protección de los datos personales.

- Si las medidas son equilibradas, proporcionando más beneficios que desventajas.

c. La representación del ciclo de vida de los datos personales a tratar.
Que implica describir las etapas del proyecto, desde su obtención, aprovechamiento, explotación, almacenamiento, conservación o cualquier otra operación realizada, hasta la supresión.

Adicionalmente, el responsable deberá especificar:

- Las fuentes (internas o externas), los medios y procedimientos a través de los cuales recabará los datos personales.

- Las áreas, grupos o personas que llevarán a cabo el tratamiento.

- Los plazos de conservación o almacenamiento.

- Las técnicas para garantizar el borrado seguro de los datos personales.

d. La identificación, análisis y descripción de la gestión de los riesgos inherentes para la protección de los datos personales.
Para cumplir con esto, la persona responsable debe crear un plan general para manejar los riesgos que identificó. Este plan debe incluir, como mínimo, lo siguiente:

- Identificar y describir de manera específica los riesgos administrativos, físicos o tecnológicos que podrían surgir al poner en marcha o modificar el proyecto.

- Evaluar qué tan probable es que ocurran los riesgos identificados y cuánto podrían afectar a las personas cuyos datos personales se están manejando.

- Establecer medidas y controles específicos que se tomarán para eliminar, reducir, transferir o manejar los riesgos detectados, asegurando que no afecten negativamente a las personas involucradas.

e. 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.

Describir los métodos o pasos que seguirá el responsable para asegurar que el proyecto 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.

Los principios de "*por defecto y diseño*" en la protección de datos personales se refieren a medidas proactivas para integrar la privacidad y seguridad de datos desde el inicio de cualquier proyecto.

Protección de datos desde el diseño: Este principio implica que la protección de datos personales debe ser una consideración integral en el desarrollo de nuevos proyectos. Esto significa que la privacidad debe ser incorporada en la tecnología misma y en todas las etapas de desarrollo, no añadida posteriormente como un elemento adicional. Por ejemplo, al diseñar una nueva aplicación, la protección de datos debería considerarse desde la fase de conceptualización, asegurando que la arquitectura de la aplicación proteja la privacidad de los usuarios por medio de técnicas como la minimización de datos (recoger solo los datos necesarios) y la encriptación.

Protección de datos por defecto: Este principio asegura que las configuraciones predeterminadas de cualquier proyecto que maneje datos personales estén configuradas para garantizar el máximo grado de privacidad. Esto significa que sin que el usuario tenga que realizar ajustes o configuraciones adicionales, sus datos ya están protegidos. Por ejemplo, una aplicación que, por defecto, tiene las cuentas configuradas como privadas en lugar de públicas, asegurando que solo el titular de la app pueda ver la información del perfil a menos que el usuario decida cambiarlo explícitamente.

f. Los resultados de la o las consultas externas que, en su caso, se efectúen.
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 del proyecto, de aquéllas que no consideró.

g. 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.
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 del proyecto.

h. 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.
Información adicional que el responsable estime apropiado someter a consideración del OGL, relacionada con el proyecto.

## 3.4. Procedimiento de la EIPD.

a. Presentación. El responsable deberá presentar la EIPD ante el OGL, al menos, *treinta días anteriores* a la fecha en que pretende poner en operación o modificar el proyecto.

b. Acuerdo. Una vez presentada la EIPD, el OGL deberá verificar que esta cumpla con los requerimientos mínimos y emitirá, dentro de los cinco días contados a partir del siguiente a la recepción de la evaluación, un acuerdo de:

- Admisión. Al cumplir con todos los requerimientos a que se refiere el artículo 14 de las Disposiciones Administrativas, o

- Requerimiento. Por una sola ocasión para que, dentro del plazo de cinco días contados a partir del siguiente a la recepción del requerimiento, cumpla

con los requisitos previstos en las Disposiciones Administrativas. En caso de no cumplir, se tendrá por no presentada la EIPD.

c. Diligencias y reuniones. El OGL podrá realizar, hasta antes de emitir su dictamen, diligencias y reuniones de trabajo con el responsable, con el objeto de contar con mayores elementos de valoración.

d. Valoración. Previo a la emisión del dictamen respectivo, el OGL deberá valorar la EIPD, para lo cual, de conformidad con las Disposiciones Administrativas, deberá tomar en cuenta los siguientes rubros:

Primero. Los objetivos generales y específicos del proyecto.
Verificando que, el objetivo general y específicos, se ajusten a un marco legal, es decir, que el tratamiento de datos personales que se pretende derive de las facultades o atribuciones que la normativa aplicable le confiera al responsable, lo anterior, en cumplimiento con el principio de licitud.

Adicionalmente, valorar si los objetivos trazados para el proyecto se apegan al principio de finalidad, debiendo estar justificados por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normativa aplicable le confiera al responsable.

En suma, estimar si el responsable definió con claridad los objetivos del proyecto y si estos se encuentran relacionados con atribuciones que expresamente le ha conferido la normativa aplicable.

Segundo. Las razones o motivos que justifican la puesta en operación o modificación del proyecto, en función de las atribuciones o facultades del responsable que la normativa aplicable le confiera.
Para ello, se debe de considerar la idoneidad, pertinencia y necesidad de la implementación o modificación del proyecto, acreditando que el tratamiento intensivo o relevante de datos personales se encuentre en función de las atribuciones legalmente atribuidas al responsable.

Tercero. Las categorías de titulares.
En relación con las categorías de titulares, estás deberán ser acordes a los objetivos y finalidad planteada para el proyecto, es decir, abarcar exclusivamente al público

involucrado. Asimismo, el responsable deberá distinguir si entre los titulares de los datos personales a tratar, se encuentran aquellos que pertenecen a grupos vulnerables en función de su edad, género, origen étnico o racial, estado de salud, preferencia sexual, nivel de instrucción, y condición socioeconómica.

Cuarto. Los datos personales tratados y su volumen.

Valorando si los datos personales resultan adecuados, relevantes y estrictamente necesarios para cumplir con los fines de su tratamiento, lo anterior, en apego al principio de responsabilidad, que obliga al responsable a llevar a cabo un manejo limitado, es decir, los datos personales, así como sus procesos de tratamiento, deberán de circunscribirse exclusivamente al cumplimiento de los fines para los cuales fueron recopilados.

Quinto. Las finalidades del tratamiento intensivo o relevante de datos personales.

Comprobando si el tratamiento que se pretende realmente tiene el carácter de intensivo o relevante, de conformidad con la normativa aplicable. Asimismo, verificar que las finalidades planteadas se encuentren en armonía con los objetivos previamente trazados para el proyecto y que estas resulten concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normativa aplicable confiere al responsable.

Sexto. Las transferencias, nacionales o internacionales, de datos personales que, en su caso, pretendan efectuarse con la puesta en operación o modificación del programa.

Para ello, se deberá valorar si dichas transferencias se encuentran motivadas por una finalidad o finalidades concretas, así como si cuentan con una periodicidad, verificando adicionalmente las categorías de datos objeto de transferencia e identificando si estos tienen un carácter sensible.

Además, considerar si las transferencias son de carácter nacional o internacional, la clase de destinatarios o terceros receptores y los medios a través de los cuál se efectuarán, comprobando las medidas de seguridad adoptadas para tal acto, así como que dichas transferencias hayan sido formalizadas mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico aplicable.

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

Respecto de la cual se debe de efectuar un estudio detallado de los aspectos técnicos del proyecto, que abarque las características del servidor, del sistema operativo, el uso del firewall, del internet, la base de datos, las medidas de seguridad, así como de los organismos certificadores que emplea el sistema sometido a la evaluación.

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

Las cuales deberán ser acordes a la naturaleza de los datos personales a tratar y del documento de seguridad elaborado para tal efecto.

En el caso de las medidas de seguridad de carácter administrativo, corroborar la existencia de políticas de seguridad, reglamentación interna o manuales de procesos, clasificación y control de activos, establecimiento de contraseñas, existencia de criterios de identificación y autentificación de personas autorizadas, establecimiento de roles y demás medidas tendentes a garantizar la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, formación y capacitación del personal, en materia de protección de datos personales.

Por lo que hace a las medidas de seguridad de carácter físico, confirmar la existencia mecanismos de acceso exclusivo a personal autorizado, de sistemas de vigilancia, programas de prevención de daños en instalaciones físicas, la existencia de mantenimiento eficaz a los equipos que almacenan datos, entre otras tendentes a proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

En el caso de las medidas de seguridad técnicas, corroborar la existencia de acceso controlado a los datos personales a través de usuarios identificados y autorizados, el establecimiento de esquemas de privilegios para realización de actividades conforme a las funciones asignadas, contemplar la revisión de la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, prever la gestión de comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento, y demás necesarias para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

Noveno. 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 del proyecto.

Verificando la existencia de una metodología concreta para gestión de riesgos potenciales en la operación del proyecto, la cual debe incluir la identificación de riesgos asociados y la implementación de medidas y controles específicos para su mitigación, así como estándares de riesgo para el tratamiento de los datos personales, respaldados a su vez se por mecanismos de seguridad, garantizando con ello el debido cumplimiento de los principios, deberes y obligaciones establecidas por las disposiciones en la materia.

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

Para lo cual se deberán identificar los riesgos, las probabilidades de que estos puedan ocurrir, las medidas a implementar en caso de que estos se actualicen y los controles específicos para prevenirlos.

Decimoprimero. Los mecanismos o procedimientos que adoptará el responsable para que el proyecto 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.

Partiendo de un análisis integral de la EIPD presentada, del cual, se pueda desprender que el diseño del sistema y su subsecuente puesta en operación se adhieren a las disposiciones legales aplicables.

Decimosegundo. La opinión técnica del oficial de protección de datos personales respecto del proyecto.

En el caso en que los responsables cuenten con un oficial de protección de datos personales este emitirá su opinión, previa solicitud, así como consideraciones técnicas, en las que aborde de manera detallada cada elemento del tratamiento intensivo o relevante que se pretende llevar a cabo.

## 3.4. Dictamen.

El OGL contará con un plazo de treinta días hábiles contados a partir del día siguiente a la recepción de la evaluación de impacto, para emitir el dictamen correspondiente, en el que, de manera fundada y motivada, determine si el proyecto:

a. **Cumple.** Apegándose a lo dispuesto en la LGPDP y demás normativa aplicable, sin necesidad de emitir recomendaciones no vinculantes al respecto, o

b. **No cumple.** Al infringir disposiciones previstas en la LGPDP y demás normativa aplicable, siendo necesario emitir recomendaciones no vinculantes al respecto.

Asimismo, a través del dictamen emitido, el OGL podrá orientar al responsable para el fortalecimiento y mejor cumplimiento de las obligaciones previstas en la LGPDP y demás disposiciones aplicables, señalando medidas, acciones y sugerencias específicas en función de las características generales y particularidades del proyecto.

Finalmente, debe señalarse que, el dictamen, no podrá tener por efecto:

a. Impedir la puesta en operación o modificación del proyecto, y

b. Validar el presunto cumplimiento de las obligaciones previstas en la LGPDP y demás disposiciones aplicables, en perjuicio de las atribuciones conferidas al OGL.

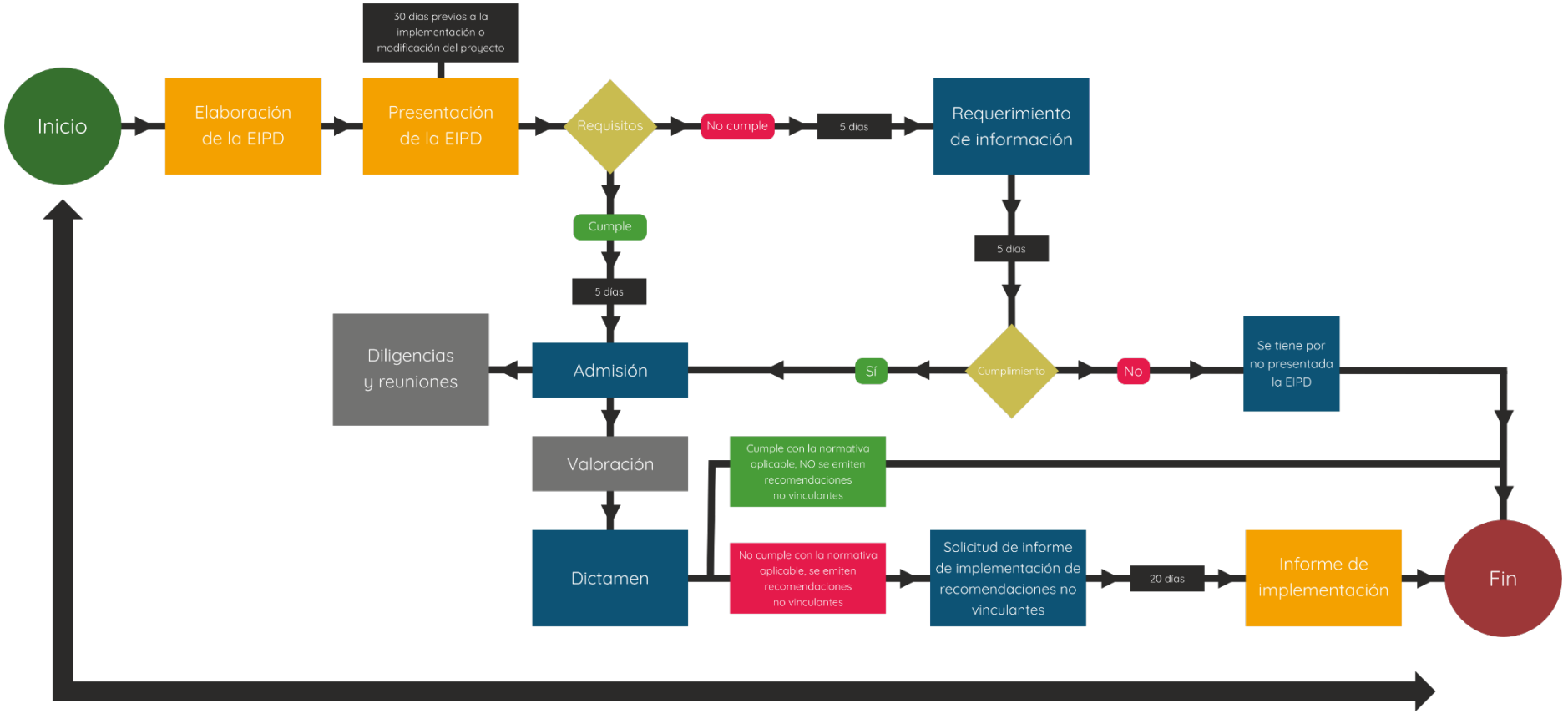
# 4. Etapas posteriores.

## 4.1. Informe de implementación.

El OGL podrá solicitar al responsable que informe sobre la implementación de las recomendaciones no vinculantes, para lo cual, otorgará en un plazo máximo de veinte días, contados a partir del día siguiente a la recepción del requerimiento.

El informe de implementación servirá al OGL para 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.

## 4.2. Mapa de proceso.



SISTEMA NACIONAL
DE TRANSPARENCIA
ACCESO A LA INFORMACIÓN PÚBLICA
Y PROTECCIÓN DE DATOS PERSONALES

REGIÓN
CENTRO
OCCIDENTE