Instituto Nacional Electoral

METODOLOGÍA PARA LA EVALUACIÓN DE IMPACTO.

EN LA PROTECCIÓN DE DATOS PERSONALES

TRANSPARENCIA y PRIVACIDAD

CONTENIDO

ACRÓNIMOS

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.

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

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

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

UTTyPDP o Unidad de Transparencia: Unidad Técnica de Transparencia y Protección de Datos Personales.

TÉRMINOS Y DEFINICIONES

Para efectos del presente documento, se tomarán las definiciones establecidas en la Ley General, en el Programa para la Protección de Datos Personales del INE y sin prejuicio de lo previsto en la normativa aplicable en la materia, se entenderá por:

Activo: En términos generales, es un bien tangible o intangible que una organización posee y que es requerido para su funcionamiento y el logro de objetivos; es decir, tiene valor para la organización.

Ciclo de vida: Las etapas de la información que contiene datos personales desde su captación hasta su borrado o conservación.

Principio de legalidad: En general, 'legalidad' significa conformidad a la ley. Se llama 'principio de legalidad' aquel en virtud del cual los poderes públicos están sujetos a la ley, de tal forma que todos sus actos deben ser conforme a la ley, bajo la pena de invalidez. Dicho de otra forma: es inválido todo acto de los poderes públicos que no sea conforme a la ley. Se entiende que esta regla se refiere especialmente -aunque no de una forma exclusiva- a los actos del Estado que pueden incidir sobre los derechos subjetivos (de libertad, de propiedad, etcétera) de la ciudadanía, limitándolos o extinguiéndolos.[1]

[1] Guastini, Ricardo, Estudios de teoría constitucional (en línea). trad. Miguel Carbonell. UNAM/Fontamara, México, 2001, pp. 117 y 124.

Proceso: Conjunto de fases sucesivas de un fenómeno natural o de una operación artificial. Conjunto de actividades mutuamente relacionadas o que interactúan, que utilizan las entradas para proporcionar un resultado previsto[2].

Riesgo: Probabilidad de que ocurra un evento (en función de que una amenaza explote una vulnerabilidad) con sus consecuencias negativas (impactos adversos)[3].

Riesgo inherente: Riesgo intrínseco al dato personal derivado del impacto negativo a la privacidad que puede causar en la persona.

[2] Gestión de Calidad. Universidad Santiago de Cali, URL: https://www.usc.edu.co/index.php/gestion-de-calidad/terminos-y-definiciones

[3] Definición obtenida de https://csrc.nist.gov/glossary/term/risk

INTRODUCCIÓN

Para elevar el nivel de protección establecido en la normativa aplicable en materia de protección de datos personales, los sujetos obligados pueden implementar acciones preventivas como los esquemas de mejores prácticas[4] y las evaluaciones de impacto.

La evaluación de impacto en la protección de datos personales, denominada como EIPD, es un proceso que tiene por objeto evaluar los riesgos que el tratamiento de los datos personales puede implicar para los titulares y que permite, en su caso, adoptar medidas legales, técnicas y administrativas para mitigarlos.[5] .

Se materializa a través de un documento elaborado por los sujetos obligados (tanto responsable como encargado del tratamiento) para identificar y mitigar dichos riesgos, relacionados con el cumplimiento de la normativa aplicable en materia de protección de datos personales, cuando pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con la Ley General impliquen el tratamiento intensivo o relevante de datos personales.[6]

A un alto nivel, una EIPD coadyuva a[7]:

- Garantizar el cumplimiento de los requisitos legales, reglamentarios, contractuales y de políticas aplicables en materia de protección de datos personales.
- Determinar de las amenazas, vulnerabilidades, efectos (daños y problemas) y riesgos resultantes.
- Evaluar las medidas y procesos alternativos para mitigar los riesgos de privacidad identificados.
- Desarrollar un proceso de priorización para implementar los procesos de mitigación y las prácticas de privacidad asociadas.

[4] Mecanismos complementarios al cumplimiento de la normativa en materia de protección de datos personales para acreditar el cumplimiento del principio de responsabilidad y rendir cuentas sobre el tratamiento de los datos personales a los titulares de datos personales como a los órganos garantes o autoridades de control. Diccionario de Protección de Datos Personales pp. 351

[5] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados comentada, pp. 228.

[6] ÍDEM, pp. 232, 233

[7] ISO/IEC 29134 First edition2017-06 Information technology – Security techniques – Guidelines for privacy impact assessment.

El INE, comprometido con la protección de los datos personales que, conforme a sus atribuciones son un insumo necesario para garantizar el ejercicio de los derechos político-electorales y contribuir al desarrollo de la vida democrática del país, ejecuta, como una buena práctica para el cumplimiento de los principios, deberes, derechos y obligaciones que establecen las normas, así como para la rendición de cuentas a las personas titulares y al Órgano Garante, considera la ejecución de evaluaciones de impacto en los tratamientos que son intensivos o relevantes.

Al respecto, la Unidad de Transparencia, en el Sistema de Gestión para la Protección de Datos Personales (SiPRODAP) Cláusula 8.3, señala que *el Instituto debe aplicar evaluaciones de impacto de datos personales para identificar los riesgos relacionados en su procesamiento, en función de los establecido en la legislación aplicable en la materia*.

Por lo que el INE debe:

a) Evaluar las consecuencias potenciales que pueden resultar si el riesgo identificado se materializa para los titulares de los datos.
b) Mantener la información documentada sobre las evaluaciones de impacto.

Para su cumplimiento, el Catálogo de controles del SiPRODAP, incluye el control “Instrumentos para llevar a cabo EIPDs”, cuyo objetivo es disponer de un instrumento que permita homologar el proceso de identificación, generación y presentación de las EIPDs,

Esta metodología tiene como finalidad contar con la información, procedimiento y formatos que permita a las áreas responsables y a la Unidad de Transparencia identificar cuándo se debe ejecutar una EIPD y cómo.

El documento está conformado por cuatro secciones:

- Parte I. Generalidades.
- Parte II. Qué es la evaluación de impacto para la protección de datos personales.
- Parte III. Fases de una EIPD.
- Parte IV. Informe de EIPD y requerimientos de información.

PARTE I. GENERALIDADES

OBJETIVO

Establecer la información, procedimiento y formatos que permitan a las áreas responsables y a la Unidad de Transparencia identificar cuándo y cómo se debe ejecutar una Evaluación de impacto en la protección de datos personales para su presentación ante el INAI, como Órgano Garante.

APLICABILIDAD

El presente documento es aplicable a los Órganos Ejecutivos, Técnicos de vigilancia, en materia de transparencia y de control, a nivel central y desconcentrado que, por sus funciones, hagan un **tratamiento intensivo o relevante de datos personales**.

REFERENCIAS NORMATIVAS

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículos 74, 75, 76, 77, 78, 79.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público (emitidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales), artículo 120.
- Disposiciones Administrativas de Carácter General para la Elaboración, Presentación y Valoración de Evaluaciones de Impacto en la Protección de Datos Personales (emitidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales).
- Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales, artículo 58.

LA EIPD Y SU RELACIÓN CON EL DOCUMENTO DE SEGURIDAD

Una de las obligaciones que las áreas responsables adquieren al tratar datos personales es la elaboración del Documento de Seguridad (en adelante Documento o DS); dentro de los apartados que lo conforman se encuentra el análisis de riesgos de los datos personales.

En el caso de que la política pública, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que de conformidad con la Ley General impliquen el tratamiento de datos personales **sea de nueva creación**, el área responsable debe ejecutar un análisis de riesgos de privacidad y datos personales.

Si como resultado de este análisis el área responsable identifica que realiza un tratamiento intensivo o relevante de datos personales, entonces, además de elaborar el DS, deberá también realizar una EIPD (a partir de la información utilizada para la conformación del Documento de Seguridad).

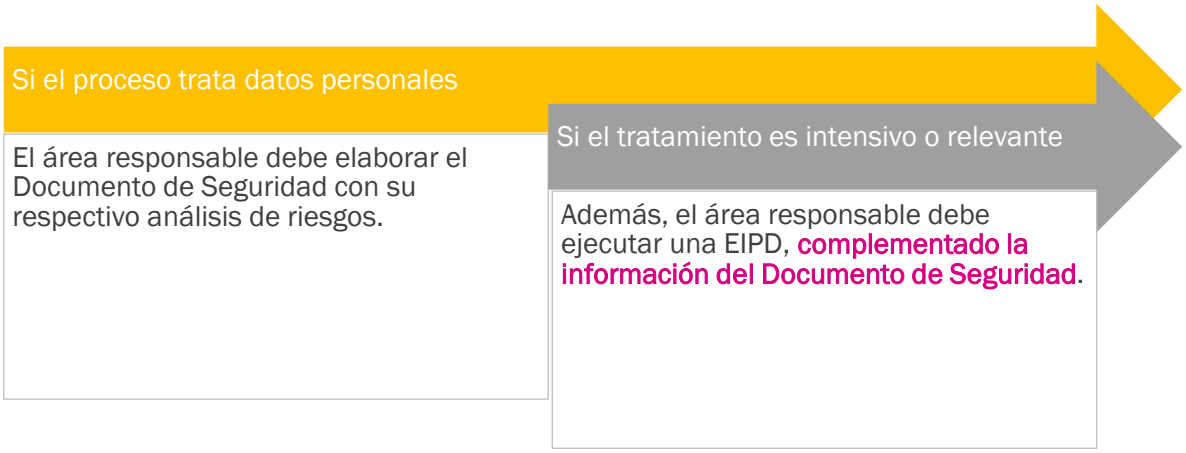

Figura 1. Documento de Seguridad y Evaluación de Impacto

La Tabla 1 presenta la relación de los elementos que son utilizados para la conformación de ambos documentos.

Tabla 1. Contenido del Documento de Seguridad vs EIPD

Apartado documento de seguridad (LGPDPPSO, Lineamientos Generales)		¿Se utiliza en la EIPD? (Disposiciones administrativas)
I.	**El inventario de datos personales y de los sistemas de tratamiento**, considerando al menos los siguientes elementos:	Sí. Artículos: • 14, fracción III, IV • 15, fracción IX, X

Tabla 1. Contenido del Documento de Seguridad vs EIPD		
	Apartado documento de seguridad (LGPDPPSO, Lineamientos Generales)	¿Se utiliza en la EIPD? (Disposiciones administrativas)
	a. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales; b. Las finalidades de cada tratamiento; c. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no; d. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales; e. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento; f. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y g. En su caso los destinatarios o terceros receptores de las trasferencias que se efectúen, así como las finalidades que justifican estas. En la elaboración del inventario de datos personales, considerar su **ciclo de vida**, considerando: a. La obtención de los datos personales; b. Su almacenamiento; c. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo sistemas físicos y/o electrónicos utilizados para tal fin; d. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso se efectúen; e. El bloque de los datos personales, en su caso, y f. La cancelación, supresión o destrucción de los datos personales. Además, se deberá **identificar el riesgo inherente de los datos personales**, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal o cualquier otro recurso humano y material que resulte pertinente considerar.	• 18
II.	**Las funciones y obligaciones de las personas que traten datos personales**. Establecer y documentar los	Sí

Tabla 1. Contenido del Documento de Seguridad vs EIPD		
	Apartado documento de seguridad (LGPDPPSO, Lineamientos Generales)	**¿Se utiliza en la EIPD? (Disposiciones administrativas)**
	roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales.	Artículo 15, fracción IX, X
III.	**El análisis de riesgos de los datos personales tratados**, considerando lo siguiente: a. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico; b. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida; c. El valor y exposición de los activos involucrados en el tratamiento de los datos personales; d. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y e. Respecto de las medidas de seguridad adoptadas, considerar, i. el riesgo inherente de los datos personales, ii. la sensibilidad de los datos personales tratados, iii. el desarrollo tecnológico, iv. las posibles consecuencias de una vulneración para los titulares, v. las transferencias de datos personales que se realicen, vi. el número de titulares, vii. las vulneraciones previas ocurridas en los sistemas de tratamiento y viii. el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.	Sí Artículo 19
IV.	**El análisis de brecha**, considerando: a. Las medidas de seguridad existentes y efectivas; b. Las medidas de seguridad faltantes, y	Sí Artículo 15, fracc. XIII

Tabla 1. Contenido del Documento de Seguridad vs EIPD		
	Apartado documento de seguridad (LGPDPPSO, Lineamientos Generales)	**¿Se utiliza en la EIPD? (Disposiciones administrativas)**
	c. La existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente.	
V.	**El plan de trabajo**, que: a. Defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer; b. Considere los recursos designados, el personal interno y externo y las fecha compromiso para la implementación de las medidas de seguridad nuevas o faltantes.	Sí Artículos: • 15, fracc. XIII • 19 • 20
VI.	**Los mecanismos de monitoreo y revisión** de las medidas de seguridad, considerando: a. Los nuevos activos que se incluyen en la gestión de riesgos; b. Las modificaciones necesarias a los activos, como podrían ser el cambio o migración tecnológica, entre otras; c. Las nuevas amenazas que podrían estar activas dentro y fuera de la organización y que no han sido valoradas; d. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes; e. Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir; f. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y g. Los incidentes y vulneraciones de seguridad ocurridas.	No aplica como una sección específica de la EIPD. Sin embargo, el monitoreo es de utilidad para identificar si se requiere realizar una EIPD derivado de una actualización o en caso de que en un primer análisis no se haya considerado necesaria su ejecución.
VII.	**El programa integral de capacitación** a corto, mediano y largo plazo que considere roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de los puestos, tomando en cuenta lo siguiente:	No aplica como una sección específica de la EIPD. Sin embargo, el programa integral de capacitación puede reportarse como medida de seguridad administrativa.

Tabla 1. Contenido del Documento de Seguridad vs EIPD	
Apartado documento de seguridad (LGPDPPSO, Lineamientos Generales)	¿Se utiliza en la EIPD? (Disposiciones administrativas)
a. Los requerimientos y actualizaciones del sistema de gestión; b. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con su tratamiento; c. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y d. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.	

PARTE II. QUÉ ES LA EVALUACIÓN DE IMPACTO EN PROTECCIÓN DE DATOS

Una evaluación de impacto es:

- Un **documento** mediante el cual el responsable valora los impactos reales respecto de un **tratamiento intensivo o relevante de datos personales**, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes, derechos y demás obligaciones en la materia.[8]

- Un **instrumento** para evaluar los impactos potenciales sobre la privacidad de un proceso, sistema de información, programa, módulo de software, dispositivo u otra iniciativa que procesa información de identificación personal y, en consulta con las partes interesadas, para tomar acciones según sea necesario para tratar el riesgo de privacidad.[9]

- Más que una herramienta; es un **proceso** que comienza en las etapas más tempranas posibles de una iniciativa, cuando todavía hay oportunidades para influir en su resultado y, por lo tanto, garantizar la privacidad por diseño. Es un proceso que continúa hasta que se implementa el proyecto, e incluso después.[10]

En una evaluación de impacto, las áreas responsables analizan cómo se recopila, usa, comparte y mantiene los datos personales en un proceso, sistema de información, programa, módulo de software, dispositivo u otra iniciativa. Al ser un proceso estructurado **permite identificar y mitigar los riesgos de privacidad** que se ejecuta en un sistema de información definido.[11]

A este respecto, es importante señalar que:[12]

a) el enfoque de riesgos utilizado en una EIPD no está solamente orientado a solventar las posibles consecuencias que, para los afectados, pudiera suponer un posible incumplimiento normativo, sino que analiza que el tratamiento se encuentre fundamentado con una base jurídica y en la evaluación del interés legítimo.

b) las medidas legales, técnicas y administrativas que pudieran plantearse como resultado de una gestión del riesgo para los derechos y libertades no justifican, por ejemplo, la inexistencia o utilización errónea de una determinada base jurídica para un tratamiento,

---

[8] Artículo 3, Fracc. XVI, LGPDPPSO.

[9] ISO/IEC 29134 First edition2017-06 Information technology – Security techniques – Guidelines for privacy impact assessment.

[10] Ídem

[11] Ídem

[12] Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. AEPD. Junio 2021.

tampoco, por ejemplo, la carencia de que concurra alguna de las excepciones que levantan la prohibición de tratar categorías especiales de datos.

c) la gestión del riesgo para los derechos y libertades tiene por objetivo el estudio del impacto y la probabilidad de causar daño a las personas, a nivel individual o social, como consecuencia de un tratamiento de datos personales. Por el contrario, la gestión de riesgo de cumplimiento normativo tiene por objetivo facilitar al responsable una herramienta para verificar el grado de cumplimiento de las obligaciones y preceptos exigidos legalmente con relación a una actividad de tratamiento.

Una vez identificados los riesgos, el siguiente paso en la EIPD es proporcionar un análisis para respaldar la toma de decisiones informada, identificar los requisitos y hacer recomendaciones sobre cómo mitigar o responder a los riesgos.[13]

Finalmente, la EIPD provee un informe que incluye documentación sobre las medidas tomadas para el tratamiento de riesgos, por ejemplo, medidas que surgen del uso del sistema de gestión de seguridad de la información (SGSI) en ISO/IEC 27001.

OBJETIVOS Y BENEFICIOS DE UNA EIPD

OBJETIVOS

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

b) Describir las acciones concretas para la gestión de los riesgos identificados;

c) Analizar y facilitar el cumplimiento de los principios, deberes, derechos y demás obligaciones previstas en la Ley General y demás disposiciones aplicables, respecto a tratamientos intensivos o relevantes de datos personales, y

d) Fomentar una cultura de protección de datos personales al interior de la organización.

BENEFICIOS

a) Identifica impactos en la privacidad, riesgos y responsabilidades.

[13] Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. AEPD. Junio 2021

b) Aporta información al diseño para la protección de la privacidad (privacidad desde el diseño);

c) Identifica los riesgos de privacidad de un nuevo sistema de información y evaluar su impacto y probabilidad (privacidad por defecto);

d) Provee las bases para identificar actualizaciones posteriores o actualizaciones con funcionalidades adicionales que puedan afectar los datos personales tratados;

e) Proporciona evidencia relacionada con el cumplimiento.

TRATAMIENTO INTENSIVO O RELEVANTE DE DATOS PERSONALES

La LGPDPPSO no define el concepto relativo al tratamiento intensivo o relevante de datos personales, sin embargo, incluye un conjunto de criterios a considerar si se está ante dichos tratamientos.[14]

Los criterios se agrupan en dos tipos de condiciones:

- Generales y
- Adicionales.

Figura 2. Criterios para determinar el tratamiento intensivo o relevante.

[14] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Comentada, INAI, noviembre 2018, pp. 230

El área responsable, con apoyo de la Unidad de Transparencia debe analizar el tratamiento con base en las condiciones para identificar si se está ante la presencia de un tratamiento intensivo o relevante.

Para tal efecto, el área responsable utilizará el Formato "Condiciones generales y adicionales", disponible en el Anexo I de este documento.

Las condiciones se explican en los siguientes apartados.

CONDICIONES GENERALES

Las áreas responsables -junto con la Unidad de Transparencia- identificarán si están en presencia de un tratamiento intensivo o relevante de datos personales, cuando concurra cada una de las siguientes condiciones[15]:

a) **Existan riesgos inherentes a los datos personales a tratar**, entendidos como el valor potencial cuantitativo o cualitativo que pudieran tener éstos para una tercera persona no autorizada para su posesión o uso en función de:

   - la sensibilidad de los datos personales;
   - las categorías de titulares involucrados;
   - el volumen total de los datos personales tratados;
   - la cantidad de datos personales que se tratan por cada titular;
   - la intensidad o frecuencia del tratamiento; o bien
   - la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas.

b) **Se traten datos personales sensibles**, entendidos como aquellos que se refieran a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleva un riesgo grave para éste. De manera enunciativa mas no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como:

   - origen racial o étnico,
   - estado de salud presente o futuro,

[15] Artículo 7 de la LGPDPPSO y 120 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

- información genética,
- creencias religiosas, filosóficas y morales,
- opiniones políticas y
- preferencia sexual

c) **Se efectúen o pretendan efectuar transferencias[16] de datos personales**, considerando con especial, de manera enunciativa mas no limitativa:

- las finalidades que motivan estas y su periodicidad prevista;
- las categorías de titulares involucrados;
- la categoría y sensibilidad de los datos personales transferidos;
- el carácter nacional y/o internacional de los destinatarios o terceros receptores y
- la tecnología utilizada para su realización.

CONDICIONES PARTICULARES

Si las áreas responsables -junto con la Unidad de Transparencia- identificaron que la política pública, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología cumple con las tres condiciones anteriores respecto del tratamiento intensivo o relevante de datos personales, entonces deben identificar si se actualiza alguna de las siguientes condiciones particulares:[17]

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

b) **Decisiones automatizadas que establezca diferencias de trato o un trato discriminatorio**. Evaluar, monitorear, predecir, describir, clasificar o categorizar la conducta o aspectos análogos de los titulares, a través de la elaboración de perfiles determinados para

[16] Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado. Artículo 3, fracc. XXXII de la LGPDPPSO.

[17] Artículo 9 de las Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.

cualquier finalidad, destinados a producir efectos jurídicos que los vinculen o afecten de manera significativa, especialmente, cuando a partir de dicho tratamiento se establezcan o pudieran establecerse diferencias de trato o un trato discriminatorio económico, social, político, racial, sexual o de cualquier otro tipo que pudiera afectar la dignidad o integridad personal de los titulares;

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

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

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

f) **Hacer coincidir o combinar conjuntos de datos**. Realizar un tratamiento frecuente y continúo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas;

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

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

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

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

k) **Datos sensibles en tratamientos masivos o sistemáticos**. Tratar datos personales sensibles con la finalidad de efectuar un tratamiento sistemático y masivo de los mismos;

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

m) **Categorías especiales**. Realizar un tratamiento a gran escala de datos personales sensibles o datos personales relativos a condenas e infracciones penales, o

n) **Monitoreo sistemático**. La observación sistemática a gran escala de una zona de acceso público.

IDENTIFICAR LA OBLIGACIÓN DE ELABORAR UNA EIPD

Las áreas responsables, junto con la Unidad de Transparencia, deben evaluar si existe la obligación de elaborar una EIPD, tomando en cuenta las siguientes consideraciones:

1. Las preguntas a continuación se pueden usar para evaluar más a fondo la necesidad de una EIPD.

    a) ¿El área responsable está **introduciendo/desarrollando/implementando** una política pública, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología **nueva o rediseñando una existente**?

        Por ejemplo:

        - Nuevos sistemas de TI o procesos manuales que implican el manejo de datos personales (recepcionista que recopila datos personales de los visitantes, eliminación de documentos físicos que contienen datos personales, presentación de reclamaciones médicas físicas, por mencionar algunas).

        - Un rediseño del flujo de trabajo de un proceso operativo que involucra a diferentes grupos de usuarios que manejan datos personales.

    b) ¿La política pública, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que el área responsable **pretende poner en operación o modificar implica un tratamiento intensivo o relevante de datos personales?**

Por ejemplo, un cambio del proceso de negocio que puede incluir la recopilación de nuevos tipos de datos personales.

- Si la respuesta es "sí" a ambas preguntas, **entonces el área responsable, con apoyo de la Unidad de Transparencia, debe realizar una EIPD.**
- Si la respuesta es "no" a alguna de las preguntas anteriores, **entonces no es obligatorio ejecutar una EIPD; opcionalmente**, el área responsable, a través de la Unidad de Transparencia, **puede solicitar una consulta al INAI.**
- Si la respuesta es "no" a ambas preguntas, **entonces no es necesario ejecutar una EIPD**. El área responsable, con apoyo de la Unidad de Transparencia, debe evaluar nuevamente cuando haya un cambio en los riesgos asociados con el tratamiento de los datos personales.

El área responsable, a través de la Unidad de Transparencia, deberá presentar la EIPD ante el INAI treinta días anteriores a la fecha en que se pretenda poner en operación la política pública, sistema, plataforma informática, aplicación electrónica o cualquier otra tecnología, a efecto de que emita las recomendaciones no vinculantes correspondientes.[18]

La Unidad de Transparencia documentará el resultado de este proceso en el Informe de EIPD.

EXENCIONES

No será necesario realizar la EIPD cuando el Comité de Transparencia[19] -de acuerdo con la información proporcionada por el área responsable a través de la Unidad de Transparencia- derivado de un análisis determine que:[20]

a) Se puedan **comprometer los efectos** que se pretenden lograr con la posible puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, o

[18] Artículo 23 de las Disposiciones Administrativas.

[19] Artículo 13, fracción II del Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales.

[20] Artículo 79 de la LGPDPPSO, artículo 33 de las Disposiciones Administrativas.

b) Se trate de situaciones de **emergencia o urgencia**.

El área responsable elaborará un **informe** que contenga, al menos lo siguiente, respecto 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:[21]

I. La denominación y los objetivos generales y específicos que persigue;

II. Las finalidades del tratamiento intensivo o relevante;

III. Las razones o motivos que le permitieron determinar que la evaluación de impacto en la protección de datos personales compromete los efectos, o bien, la situación de emergencia o urgencia que hacen inviable la presentación de ésta;

IV. Las consecuencias negativas que se derivarían de la elaboración y presentación de la EIPD;

V. El fundamento legal que habilitó el tratamiento de datos personales;

VI. La fecha en que se puso en operación o modificó, así como su periodo de duración;

VII. La opinión técnica del oficial de protección de datos personales -o en su caso, de la Unidad de Transparencia- respecto del tratamiento intensivo o relevante de datos personales, y

VIII. Los mecanismos o procedimientos adoptados por el área responsable para su cumplimiento, desde el diseño y por defecto, con todas las obligaciones previstas en la LGPDPPSO y demás disposiciones aplicables.

Para su elaboración, el área responsable utilizará el Formato "Informe de exención EIPD", disponible en el Anexo II de este documento.

Además, si la justificación del tratamiento responde a una situación de urgencia -casos de interés público que respondan a temas de seguridad nacional o de salud-, deberá incorporar medidas para monitorizar la vigencia de las circunstancias que justificaron el tratamiento, para reevaluar su idoneidad y licitud.

El área responsable, a través de la Unidad de Transparencia, **presentará el Informe de exención en el domicilio del INAI dentro de los treinta días posteriores a la fecha de la puesta en operación**

[21] Artículo 34 de las Disposiciones Administrativas.

o modificación de la política pública, sistema, plataforma informática, aplicaciones electrónicas o cualquier otra tecnología.[22]

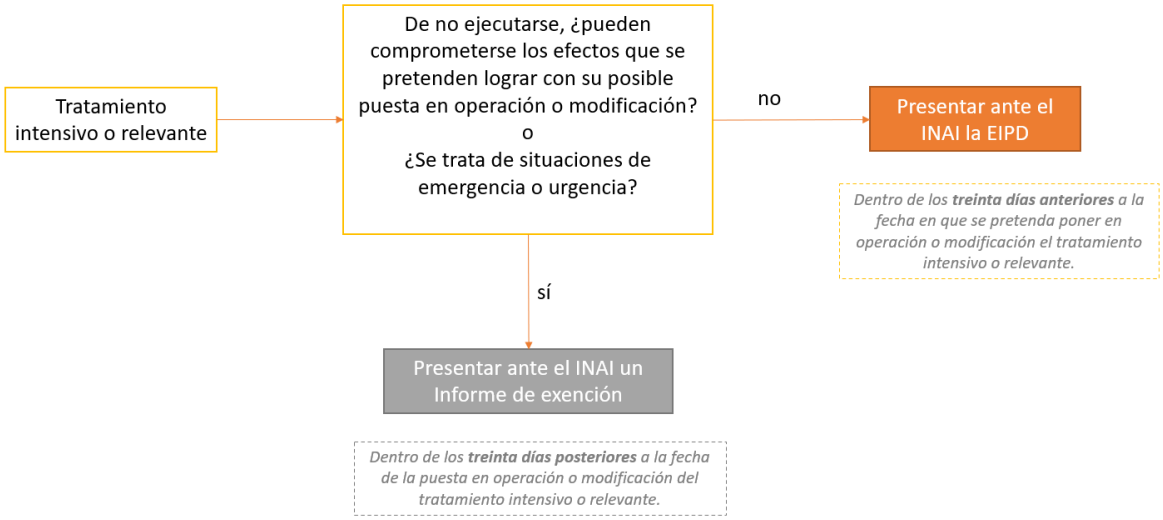

Figura 3. Cuándo presentar una EIPD o un Informe de exención

[22] Artículo 34 de las Disposiciones Administrativas.

PARTE III. FASES DE UNA EIPD

Una vez identificada la procedencia de la EIPD, su ejecución consta de nueve fases:

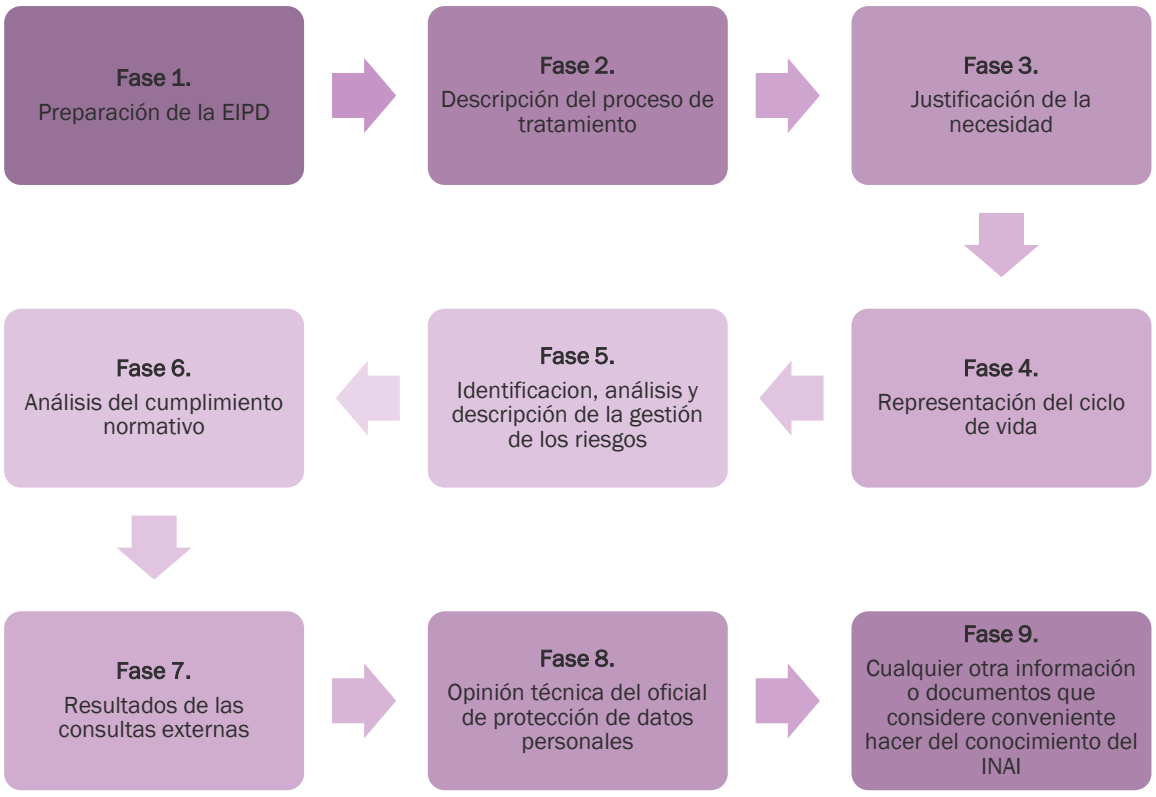

Figura 4. Fases de la EIPD

FASE 1. PREPARACIÓN DE LA EIPD

Una vez identificada la necesidad de ejecutar la EIPD, el área responsable y la Unidad de Transparencia deben:

- Especificar el alcance.
- Conformar el equipo EIPD.

Para su elaboración, el área responsable utilizará el Formato "Preparación de la EIPD", disponible en el Anexo III de este documento.

En los siguientes apartados se describen estos puntos.

ESPECIFICAR EL ALCANCE

El objetivo de esta actividad es determinar el alcance de la EIPD y los criterios de riesgo.

La Unidad de Transparencia y el área responsable deben definir el alcance del EIPD que, de manera enunciativa mas no limitativa, puede contemplar:

a. Un proceso;

b. Un sistema de información, diseñado para soportar un proceso definido;

c. Un programa, siendo un conjunto de procesos;

d. Otra iniciativa, que tiene un propósito definido;

e. Un módulo de software o un dispositivo, ya sea:

- destinado a convertirse en un subsistema del sistema de información definido en b), o
- independiente de un sistema de información dedicado, con respecto a casos de uso definidos que determinan un propósito específico de procesamiento.

La Unidad de Transparencia documentará el resultado de esta fase en el Informe de EIPD.

CONFORMAR EL EQUIPO EIPD

La Tabla 2 describe la conformación del equipo, así como sus respectivas responsabilidades.

Tabla 2. Conformación del equipo EIPD

Órganos	Personal	Responsabilidades
Unidad de Transparencia	De la Subdirección de Gobierno de Datos Personales	1. Ejecutar la EIPD. 2. Apoyar al área responsable en la definición de los criterios de riesgo. 3. Apoyar al área responsable en la identificación de los criterios para la aceptación del riesgo. 4. Documentar la ejecución de la EIPD. 5. Elaborar el Informe de EIPD.

Tabla 2. Conformación del equipo EIPD		
Órganos	**Personal**	**Responsabilidades**
Órganos del Instituto	Del área responsable.	1. Proveer toda la información que la Unidad de Transparencia solicite. 2. Analizar y validar los criterios de riesgo. 3. Analizar y validar los criterios de aceptación del riesgo. 4. Revisar el Informe de EIPD.
	De áreas custodias (Tecnologías de la información, sistemas, archivo, entre otras).	1. Proveer toda la información que el área responsable solicite.

La Unidad de Transparencia documentará el resultado de esta fase en el Informe de EIPD.

FASE 2. DESCRIPCIÓN DEL PROCESO DE TRATAMIENTO

Esta fase se refiere 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.[23]

Para ello, las áreas responsables llevarán a cabo las siguientes actividades, que son descritas en las subsecuentes secciones:

- Análisis preliminar.
- Identificación de información obligatoria.
- Identificación de información adicional en caso de EIPD interinstitucionales.

La Unidad de Transparencia documentará el resultado de esta fase en el Informe de EIPD.

ANÁLISIS PRELIMINAR

Como punto de partida, la ejecución de una EIPD requiere tener **conocimiento detallado del procesamiento a analizar**. Para ello, el área responsable debe proporcionar a la UTTyPDP

[23] Artículo 14 de las Disposiciones Administrativas.

información que le permita identificar cómo se recopilan, utilizan o divulgan los datos personales y cuál es el marco normativo que regula su tratamiento.

Para tal efecto el área responsable debe proporcionar a la Unidad de Transparencia, a través de los medios que esta determine para tal fin, al menos:

- Normativa.
- Manuales.
- Contratos con terceros.
- Informes.
- Especificaciones funcionales del sistema.
- Pruebas de seguridad

La UTTyPDP también podrá consultar de manera directa al área responsable para garantizar la exhaustividad y la precisión de la información, a través de reuniones a distancia o correo electrónico[24].

Como resultado de esta etapa la Unidad de Transparencia debe obtener:

- La descripción sistemática de las operaciones de tratamiento involucradas, la naturaleza, el ámbito, el contexto y los fines del tratamiento.
- Una visión detallada que facilite la identificación de amenazas y riesgos de datos personales.
- Descripción clara de los elementos que intervienen en cada fase del ciclo de vida.

IDENTIFICACIÓN DE INFORMACIÓN OBLIGATORIA

El área responsable, con apoyo de la Unidad de Transparencia, elaborará una **descripción detallada y objetiva** 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 contendrá, al menos[25]:

I. Antecedentes. Incluyendo la fecha en la que se pretenda poner en operación y si es un proyecto nuevo o una modificación, es decir, la implementación o algún ajuste de un

[24] Haciendo uso de los mecanismos institucionales disponibles para tal fin.

[25] Artículos 14 y 15 de las Disposiciones administrativas.

supuesto particular. En caso de una modificación o ajuste, incluir una explicación amplia de la forma en que se ejecuta el tratamiento previo a su actualización

II. Denominación, incluyendo si constituye una política pública, programas, sistemas o plataformas informáticas, aplicación electrónica o cualquier otra tecnología.

III. Nombre.

IV. Objetivos generales y específicos, descritos ampliamente.

V. Fundamento legal, conforme a sus facultades o atribuciones, descritos ampliamente.

VI. Categorías de las personas titulares, -grupos vulnerables en función de su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica-.

VII. Datos personales objeto de tratamiento, distinguiendo, en su caso, los datos personales sensibles.

VIII. Finalidades del tratamiento.

IX. Descripción puntual de los procesos, fases o actividades operativas que involucren el tratamiento de datos personales, descritos ampliamente, acompañándose de diagramas de flujo en el que sea posible apreciar su funcionamiento y las fases o procesos de los cuales se componen.

X. Forma en que se recaban los datos personales o, en su caso, las fuentes de las cuales provienen,

XI. Transferencias de datos personales que, en su caso, se efectúen o pretendan efectuarse y sus finalidades; señalar si celebrará algún convenio de colaboración o contractual, identificando la fase operativa en la que se llevará a cabo su celebración, las partes convenientes o contratantes, las condiciones convenidas o contratadas, la fecha de vigencia y, en general, todas las condicionantes que, para tal efecto, se establezcan.

XII. Tiempo de duración del tratamiento.

XIII. Tecnología que se pretende utilizar o se utiliza para llevar a cabo el tratamiento, especificando:

- todos los requerimientos técnicos de software y hardware de los elementos que los componen;
- los diagramas, esquemas, representaciones simbólicas y/o descripciones que permitan conocer a detalle elementos técnicos;

- la información que permita identificar la arquitectura en la que se desarrollan los componentes de conexión;
- el área en particular del INE que desarrolló, implementó y/o realizó el mantenimiento y operación, o si intervino o intervendrá un proveedor externo para estos servicios. En caso de la intervención de un proveedor externo incorporar los contratos de servicio, diagramas, imágenes, esquemas o descripciones detalladas que permitan identificar la funcionalidad de los elementos que comprenden el desarrollo informático, la descripción de elementos mínimos en hardware y software para el funcionamiento de la tecnología, así como las especificaciones de conexión del lado del usuario y del servidor,
- la identificación de la tecnología para identificar las necesidades de seguridad a partir de su desarrollo.
- la documentación, información y descripción de la funcionalidad y características sobre los módulos que la integran, en caso de aplicar.
- información sobre la interoperabilidad acceso y/o comunicación entre los sistemas a los que conecta
- en caso de tratarse de un sistema o plataforma informática, aplicación electrónica y de considerarlo viable, compartir en un ambiente de pruebas, usuario y contraseña a fin de proveer acceso y advertir el ambiente en el que se desarrolla, su funcionamiento y constatar las etapas, datos y demás elementos. En caso contrario, se deberán integrar pantallas de diseño de la aplicación para identificar las vistas y navegación entre las pantallas de uso.

XIV. Medidas de seguridad de carácter físico, técnico y administrativo, en materia de protección de datos personales implementadas. Este requerimiento debe estar sustentado en el análisis de brecha, del Documento de Seguridad.

XV. Nombre y cargo de las personas servidoras públicas que cuentan con facultad expresa para decidir, aprobar o autorizar la puesta en operación o modificación del tratamiento, y

XVI. Cualquier información o documentos que considere conveniente hacer de conocimiento al INAI.

Para tal efecto, el **área responsable debe elaborar un documento con base en el Formato "Identificación de información obligatoria", disponible en el Anexo IV de este documento.**

IDENTIFICACIÓN DE INFORMACIÓN ADICIONAL EN CASO DE EIPD INTERINSTITUCIONALES

En caso de que en la EIPD intervenga otro sujeto obligado, la Unidad de Transparencia documentará lo siguiente:[26]

I. La denominación de los responsables conjuntos que presentan la EIPD;

II. La denominación del responsable líder del proyecto que tendrá a su cargo coordinar las acciones necesarias entre los distintos responsables para la elaboración de la EIPD, y

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

Para tal efecto, el **área responsable debe elaborar un documento con base en el Formato "Identificación de información adicional", disponible en el Anexo V de este documento.**

FASE 3. JUSTIFICACIÓN DE LA NECESIDAD

En esta fase, el área responsable, con apoyo de la Unidad de Transparencia, debe elaborar la justificación señalando las **razones o motivos 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.[27]

Para ello, deberá garantizar el derecho a la protección de datos personales de sus titulares, considerando si la medida o medidas -*entendiéndose como medida el tratamiento que realizará a través de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se pretende implementar*-[28] propuestas son[29]:

I. **Susceptibles o idóneas**;

II. **Las estrictamente necesarias**, en el sentido de ser las más moderadas, y

III. **Equilibradas**, en función del mayor número de beneficios o ventajas que perjuicios.

[26] Artículo 16 de las Disposiciones administrativas.

[27] Artículo 17 de las Disposiciones administrativas.

[28] Análisis realizado por la Unidad de Transparencia debido a la carencia de una definición en la normativa aplicable en materia de datos personales.

[29] Artículo 17 de las Disposiciones administrativas.

Tabla 2. Evaluación de la necesidad y proporcionalidad	
Criterios	**Evaluar si**
Susceptibles o idóneas	El tratamiento es adecuado para el fin que persigue, es decir, si el tratamiento responde a determinadas carencias, demandas, exigencias, obligaciones u oportunidades objetivas y puede conseguir objetivos propuestos con la eficacia suficiente (determinar si resuelve las carencias).[30]
Las estrictamente necesarias	La finalidad perseguida no puede alcanzarse de otro modo menos lesivo o invasivo, es decir, no existe un tratamiento alternativo que sea igualmente eficaz para el logro de la finalidad perseguida.[31]
Equilibradas (proporcionales)	La gravedad del riesgo de tratamiento para los derechos y libertades, y su intromisión en la privacidad, es adecuada y proporcional al objetivo perseguido, es decir, se debe ponderar el beneficio que el tratamiento, desde el punto de vista de protección de datos, proporciona a la sociedad, manteniendo un equilibro con el impacto que representa sobre otros derechos fundamentales.[32]

El área responsable, con apoyo de la Unidad de Transparencia, debe considerar durante la evaluación de la idoneidad, necesidad y proporcionalidad el **equilibrio con otros derechos que, pueden verse afectados**, como pueden ser:[33]

- A la vida.
- A la integridad de la persona.
- A la libertad y la seguridad.
- A la libertad de expresión.
- A la libertad de profesión.
- A la libertad de propiedad, incluyendo la propiedad intelectual.
- El derecho de acceso a documentos.

Como resultado de esta evaluación el área responsable decidirá llevar a cabo o no el tratamiento, o en su caso, modificarlo para que cumpla con los criterios de la Tabla 2.

Sin embargo, **en caso de que el tratamiento no supere la evaluación, la UTTyPDP sugiere no llevar a cabo el tratamiento**, debido a que es un requisito establecido en la normativa en materia

[30] Juicio de idoneidad.

[31] Juicio de necesidad.

[32] Juicio de proporcionalidad en sentido estricto.

[33] EDPS. Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. December 2019. pp. 3

de protección de datos personales y que no puede sustituirse con medidas compensatorias o alternativas, como pueden ser las de seguridad.

Para justificar la necesidad, **el área responsable debe elaborar un documento con base en el "Formato Justificación de la necesidad", disponible en el Anexo VI.** El contenido de este documento deberá contener el resultado de las acciones que se observan en la Figura 4 y que se describen en los apartados siguientes.

La Unidad de Transparencia documentará el resultado de esta fase en el Informe de EIPD.

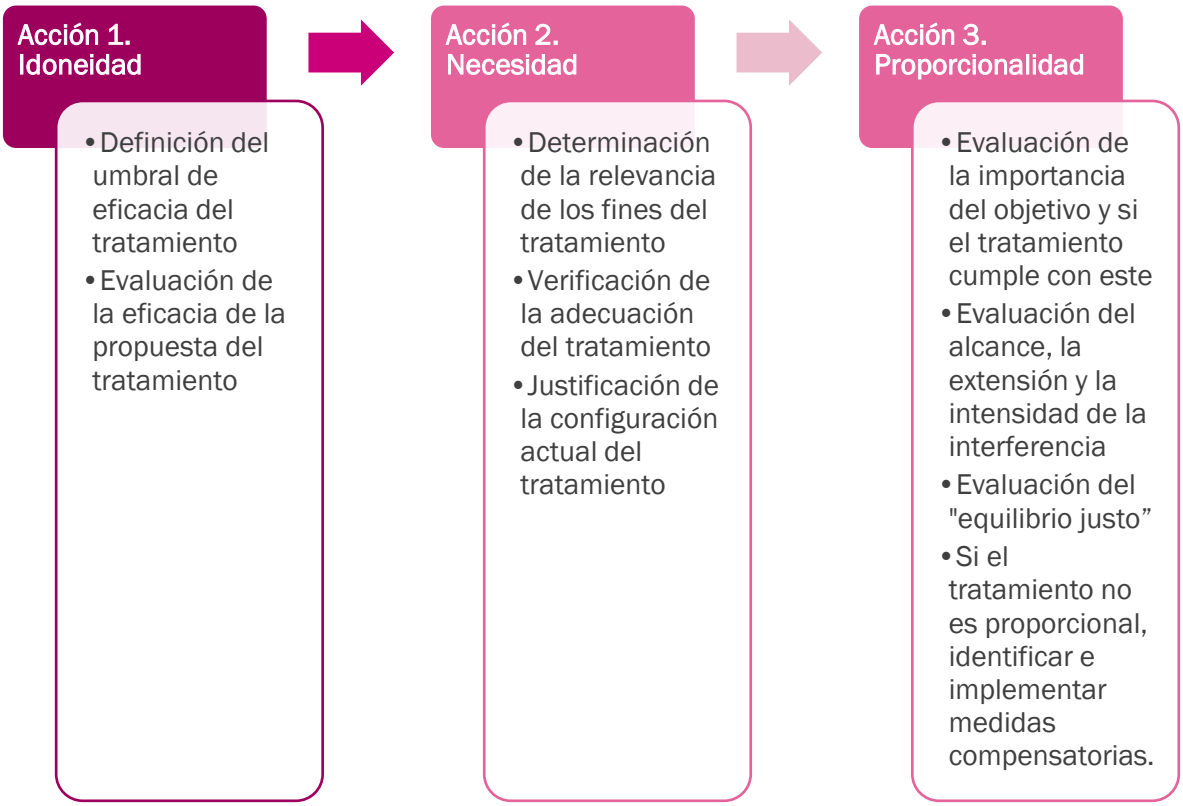

Figura 4. Acciones para evaluar la necesidad.

ACCIÓN 1. EVALUACIÓN DE LA IDONEIDAD

Para evaluar la idoneidad, el área responsable, con apoyo de la Unidad de Transparencia, debe evaluar si la propuesta de tratamiento tiene la eficacia para cumplir con los fines que persigue, la cual debe ser demostrada de forma objetiva.

Los pasos se describen en la Figura 5 y se desarrollan en la Tabla 3.

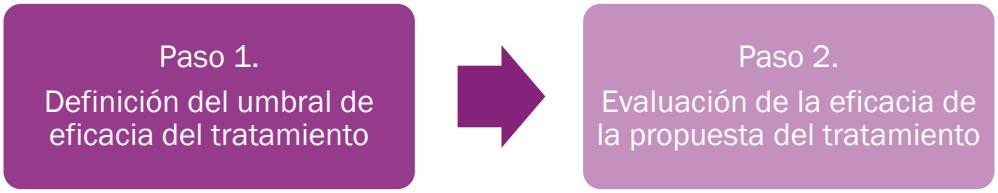

Figura 5. Pasos para evaluar la idoneidad

Tabla 3. Pasos para evaluar la idoneidad		
Paso	**Actividad**	**Ejemplo**
1. Definición del umbral de eficacia del tratamiento.	Establecer la eficacia que se debería alcanzar para cumplir con los fines del tratamiento.	Posibilidad de fraude por debajo del 1%
2. Evaluación de la eficacia de la propuesta del tratamiento.	Verificar si la propuesta de tratamiento responde a las necesidades planteadas.	Evaluar, basado en evidencias, si el fraude bajará por dejado del 1%.

La evaluación de la idoneidad debe ser racional, analítica y basada en hechos y datos objetivos.[34]

ACCIÓN 2. EVALUACIÓN DE LA NECESIDAD

Para evaluar la necesidad, el área responsable debe **considerar el principio de legalidad** -como garantía del derecho humano de protección de datos personales - así como los **principios de licitud y proporcionalidad** -en el tratamiento de datos personales-.

[34] EDPS. Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. December 2019. pp 141

Los pasos se describen en la Figura 6 y se desarrollan en la Tabla 4.

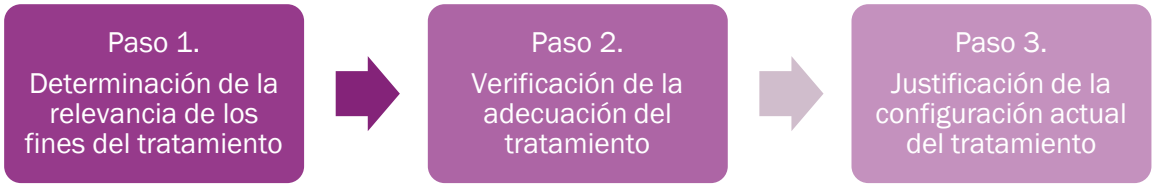

Figura 6. Pasos para evaluar la necesidad

Tabla 4. Pasos para evaluar la necesidad

Paso	Descripción	Preguntas de apoyo
1. Determinación de la relevancia de los fines del tratamiento.	Evaluar que los fines del tratamiento tienen la importancia suficiente para ser abordados con un tratamiento de alto riesgo.	¿Cuál es la base legal para el procesamiento? ¿Existe una limitación de los derechos a la privacidad y a la protección de datos personales, y posiblemente también de otros derechos?
2. Verificación de la adecuación del tratamiento.	Verificar que cada una de las operaciones del tratamiento están orientadas a cumplir con los fines de una forma objetivamente demostrable.	¿Existen otros posibles tratamientos alternativos que utilicen medios menos intrusivos y que alcancen, al menos, igual eficacia?
3. Justificación de la configuración actual del tratamiento.	Evaluar que no existen otros tratamientos, que ya están en curso o que se podrían plantear, que resuelven los fines declarados sin incurrir en un alto riesgo, incluso aunque sea necesario introducir alguna modificación para cumplir los fines perseguidos.	¿La finalidad perseguida se puede conseguir por otros medios? ¿Se ha asegurado de que se utilice la cantidad mínima de datos personales para lograr sus objetivos (minimización de datos)? ¿Es posible utilizar datos de distinta naturaleza o anonimizados? ¿Es posible usar tecnologías menos invasivas? ¿Se ha analizado si con modificaciones menores de tratamientos existentes es posible cubrir las necesidades?

ACCIÓN 3. EVALUACIÓN DE LA PROPORCIONALIDAD

La evaluación de la proporcionalidad del tratamiento con relación a sus fines no debe confundirse con la obligación de utilizar únicamente los datos que fueran adecuados, pertinentes y limitados para la finalidad del tratamiento.

El principio de proporcionalidad dispone que el procesamiento de datos será proporcionado en relación con el fin legítimo perseguido y reflejará en todas las etapas del procesamiento un justo equilibrio entre todos los intereses involucrados, ya sea público o privado, y los derechos y libertades en juego.[35]

Para evaluar la proporcionalidad, seguir los pasos se describen en la Figura 7 y se desarrollan en la Tabla 5.[36]

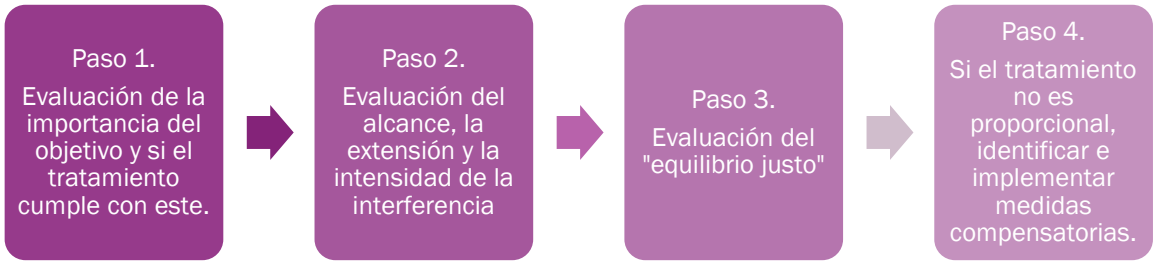

Figura 7. Pasos para evaluar la proporcionalidad

Tabla 5. Pasos para evaluar la proporcionalidad

Paso	Consideraciones o preguntas de apoyo
1. Evaluación de la importancia del objetivo y si el tratamiento cumple con este.	a) Los datos personales sólo se traten si la finalidad no se puede hacer razonablemente por otros medios, es decir, sin tratar datos personales. b) Las finalidades tienen que estar definidas de manera determinada, explícita y legítima. c) Cualquier tratamiento de datos personales tiene que ser lícito y leal. d) Los datos personales tienen que ser adecuados, pertinentes y limitados a lo necesario para los fines para los cuales se tratan. e) El plazo de conservación se limite a un mínimo estricto.
2. Evaluación del alcance, la extensión y la intensidad de la interferencia.	a) ¿Cuántas personas se verían afectadas? b) ¿Qué tipo de datos se tratarían? c) ¿Por cuánto tiempo?

[35] Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. European Data Protection Supervisor. December 2019.

[36] Ídem.

Tabla 5. Pasos para evaluar la proporcionalidad	
Paso	**Consideraciones o preguntas de apoyo**
	d) ¿permitiría la medida extraer conclusiones precisas sobre la vida privada de las personas?
3. Evaluación del "equilibrio justo".	a) Analizar los "beneficios" como de los "costos" del tratamiento; *entendiéndose por costo el riesgo al que se expondrán los datos, derivado del tratamiento o las consecuencias por una posible vulneración.* b) ¿El tratamiento previsto para cumplir el objetivo requerido es una respuesta proporcionada a la necesidad en la base de una propuesta lícita y legítima, considerando las limitaciones a la protección de datos y la privacidad?
4. Si el tratamiento no es proporcional, identificar e implementar medidas compensatorias.	a) La posibilidad de reducción del alcance o extensión del procesamiento de datos personales, su categoría y cantidad; b) Prever e introducir salvaguardas que reduzcan el impacto de la propuesta sobre los derechos fundamentales que se encuentren relacionados. c) La integración de una cláusula de extinción o un plazo de expiración (limitar el periodo de procesamiento). d) Mecanismos de supervisión.

FASE 4. REPRESENTACIÓN DEL CICLO DE VIDA DE LOS DATOS PERSONALES A TRATAR

El área responsable debe **describir y representar** cada una de las fases de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, **especificando el ciclo de vida** de éstos **a partir de su obtención, aprovechamiento, explotación, almacenamiento, conservación o cualquier otra operación realizada, hasta la supresión**.[37]

El área responsable debe identificar respecto de los datos personales:[38]

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

II. Las áreas, grupos o personas que llevarán a cabo operaciones específicas para su tratamiento;

III. Los plazos de conservación o almacenamiento, y

[37] Artículo 18 de las Disposiciones Administrativas.

[38] Ídem

IV. Las técnicas a utilizar para garantizar su borrado seguro.

Para tal efecto, la descripción y representación que realizará el área responsable tomará como base:

a) **Descripción**: del ciclo de vida mediante los Formatos "**Inventario de datos personales" disponible en el Anexo VII** de este documento.

b) **Representación**: elaboración del "**Diagrama ciclo de vida**", con base en los criterios del **Anexo VIII** y considerando el **Modelo de Ciclo de Vida de la Información**, disponible en el **Anexo IX** de este documento.

Si el área responsable cuenta con el Documento de Seguridad, la información debe tomarse de este.

La Unidad de Transparencia documentará el resultado de esta fase en el Informe de EIPD.

FASE 5. IDENTIFICACIÓN, ANÁLISIS Y DESCRIPCIÓN DE LA GESTIÓN DE LOS RIESGOS PARA LA PROTECCIÓN DE LOS DATOS PERSONALES

El área responsable, con apoyo de la Unidad de Transparencia, debe incluir la **gestión de riesgos** que tenga por objeto identificar y analizar los posibles riesgos y amenazas, así como los daños o consecuencias que pudieran producirse o presentarse si llegasen a materializarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.[39]

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

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

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

[39] Artículo 19 de las Disposiciones Administrativas.

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

Para tal efecto, el área responsable, con apoyo de la Unidad de Transparencia, elaborará un ***Informe de riesgos de privacidad y datos personales, así como el Plan de gestión de riesgos***, utilizando la ***Metodología de Análisis de Riesgos de Privacidad y Datos Personales*** del Instituto Nacional Electoral**, disponible en el Anexo X de este documento.**

Si el área responsable cuenta con el Documento de Seguridad, la información debe tomarse de este.

La Unidad de Transparencia documentará el resultado de esta fase en el Informe de EIPD.

FASE 6. ANÁLISIS DEL CUMPLIMIENO NORMATIVO

El área responsable, con apoyo de la Unidad de Transparencia, **deberá señalar los mecanismos o procedimientos adoptados para que** la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que pretende implementar o modificar y que implique un tratamiento intensivo o relevante de datos personales **cumpla, por defecto y diseño, con los principios, deberes, derechos y demás obligaciones** previstas en la Ley General y demás disposiciones aplicables.[40]

Para tal efecto, e**l área responsable debe elaborar un documento con base en el Formato Análisis de cumplimiento normativo", disponible en el Anexo XI,** que contenga el análisis con base en los apartados siguientes para identificar los controles de privacidad de acuerdo con las:

- Estrategias aplicadas para la privacidad desde el diseño.
- Estrategias aplicadas para la privacidad por defecto.

La Unidad de Transparencia documentará el resultado de esta fase en el Informe de EIPD.

A continuación, el desarrollo de cada una de las estrategias.

ESTRATEGIAS APLICADAS PARA PRIVACIDAD DESDE EL DISEÑO

[40] Artículo 20 de las Disposiciones Administrativas.

Los requisitos de privacidad[41] considerados desde las primeras etapas del diseño de las políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología son descritos en la Tabla 5, las cuales contemplan las garantías para la protección de los derechos y libertades de las personas titulares con relación a sus datos personales.

Tabla 5. Privacidad desde el diseño			
Estrategia	**Objetivo**	**Controles de privacidad**	**Ejemplos**
Minimizar	Recoger y tratar la mínima cantidad de datos posible, evitando el procesamiento de datos que no sean necesarios para las finalidades perseguidas en el tratamiento, limitando los posibles impactos en la privacidad.	• **Seleccionar**: elegir únicamente la muestra de individuos relevante y los atributos necesarios siguiendo una actitud conservadora al establecer el criterio de selección y realizar el tratamiento únicamente sobre los datos que respondan a dicho criterio (lista blanca). • **Excluir**: es el enfoque inverso al anterior, y consiste en excluir de antemano los sujetos y atributos que resulten irrelevantes para el tratamiento realizado (lista negra). En este caso se debe adoptar una actitud abierta, intentando excluir el máximo posible de registros a menos que pueda justificarse que son absolutamente necesarios para la finalidad perseguida. • **Podar**: eliminar parcialmente los datos personales tan pronto dejen de ser necesarios lo cual supone determinar de antemano cuál es el periodo de conservación	• Anonimización • Seudonimización • Bloqueo de correlación en sistemas de gestión de identidad federada

[41] Para efectos de este documento protección de datos desde el diseño y privacidad desde el diseño son considerados equivalentes.

Tabla 5. Privacidad desde el diseño			
Estrategia	**Objetivo**	**Controles de privacidad**	**Ejemplos**
		para cada uno de los datos recogidos y establecer mecanismos automáticos de borrado cuando se cumpla dicho plazo. En el caso de que los datos formen parte de un registro en el que figure más información que sea necesario conservar, el valor de los campos no necesarios puede modificarse a un valor por defecto prefijado. • **Eliminar**: suprimir por completo los datos personales tan pronto dejen de ser relevantes asegurándose que no es posible su recuperación ni siquiera de las copias de seguridad realizadas.	
Ocultar	Limitar la exposición de los datos, estableciendo las medidas necesarias para garantizar la protección de los objetivos de confidencialidad y desvinculación	• **Restringir**: gestionar de forma restrictiva el acceso a los datos personales limitándolo mediante una política de control de acceso que implemente el principio de "need to know" tanto en espacio (detalle y tipo de datos accedidos) como en tiempo (etapas del tratamiento). • **Ofuscar**: hacer que los datos personales sean ininteligibles para aquellos que no estén autorizados a su consulta utilizando técnicas de cifrado y hashing, tanto en operaciones de almacenamiento como de transmisión de la información.	• Cifrado • Redes de mezcla • Atributos basados en credenciales

Tabla 5. Privacidad desde el diseño			
Estrategia	**Objetivo**	**Controles de privacidad**	**Ejemplos**
		• **Disociar**: eliminar la vinculación entre conjuntos de datos que se han de mantener independientes, así como los atributos identificativos de los registros de datos para evitar correlaciones entre ellos, con especial atención a los metadatos. • **Agregar**: Agrupar la información relativa a varios sujetos utilizando técnicas de generalización y supresión para evitar así correlaciones.	
Separar	Evitar, o al menos minimizar, el riesgo de que, durante el procesamiento, en una misma entidad, de diferentes datos personales pertenecientes a un mismo individuo y utilizados en tratamientos independientes, se pueda llegar a realizar un perfilado completo del sujeto. Para ello, es necesario mantener contextos de tratamiento independientes que dificulten la correlación de grupos de datos que deberían estar desligados.	• **Aislar**: recoger y almacenar los datos personales en diferentes bases de datos o aplicaciones que sean independientes desde el punto de vista lógico o incluso que se ejecuten sobre sistemas físicos distintos, adoptando medidas adicionales para garantizar esa desvinculación como el borrado programado de tablas de indexación entre bases de datos • **Distribuir**: diseminar la recogida y el tratamiento de los diferentes subconjuntos de datos personales correspondientes a diferentes tipos de tratamiento sobre unidades de tramitación y gestión que, dentro de la organización, sean físicamente independientes y utilicen sistema y aplicaciones distintos intentando implementar arquitecturas	• Listas negras anónimas • Cifrado homomórfico • Separación física y lógica

Tabla 5. Privacidad desde el diseño			
Estrategia	**Objetivo**	**Controles de privacidad**	**Ejemplos**
		descentralizadas y distribuidas con procesamiento local de la información siempre que sea posible en lugar de soluciones centralizadas con accesos unificados y que dependan de una misma unidad de control.	
Abstraer	Limitar al máximo el detalle de los datos personales que son tratados. A diferencia de la estrategia 'minimizar' que realiza una selección previa de los datos recogidos, esta estrategia se centra en el grado de detalle con el que los datos son tratados y en su agregación	• **Sumarizar**: generaliza los valores de los atributos utilizando intervalos o rangos de valores, en lugar de utilizar el valor concreto del campo. • **Agrupar**: agrega la información de un grupo de registros en categorías en lugar de utilizar la información detallada de cada uno de los sujetos que pertenecen al grupo trabajando con los valores medios o generales. • **Perturbar**: utilizar valores aproximados o modificar el dato real mediante el empleo de algún tipo de ruido aleatorio en lugar de trabajar con el valor exacto del dato personal.	• Agregación en el tiempo • K-anonimidad • Ofuscación de medidas mediante agregación de ruido • Granularidad dinámica de ubicación • Privacidad diferencial
Informar	Implementación del principio de trasparencia y persigue que los interesados estén plenamente informados del procesamiento de sus datos en tiempo y forma. Siempre que se realice un tratamiento, los sujetos cuyos datos son tratados deberían conocer qué	• **Facilitar**: suministrar a los interesados toda la información exigida por la LGPDPPSO en relación con qué datos personales son tratados, cómo se procesan y por qué, mediante la identificación del motivo y finalidad. Se debe proporcionar detalles en relación con los plazos de conservación de los datos, así como de las comunicaciones de estos	• Notificación de brechas de privacidad • Visualización dinámica de la política de privacidad • Iconos de privacidad • Alertas de tratamiento

Tabla 5. Privacidad desde el diseño			
Estrategia	**Objetivo**	**Controles de privacidad**	**Ejemplos**
	información es la que se procesa, con qué propósito y a qué terceras partes es comunicada además del resto de información tratada.	que se realicen a terceras partes. Junto a toda esta información, que debe ser fácilmente accesible y proporcionarse de forma continuada en el tiempo para fomentar una auténtica trasparencia, debe indicarse también con quién y cómo pueden ponerse en contacto los sujetos de datos para plantear cuestiones relativas a su privacidad, así como los derechos que les asisten en materia de protección de datos personales • **Explicar**: facilitar la información relativa a los tratamientos de forma concisa, transparente, inteligible y de fácil acceso utilizando un lenguaje claro y sencillo. Para evitar avisos de privacidad densos y complejos conviene adoptar una aproximación por capas o niveles en la que se presente una información básica, en un primer nivel y de forma resumida, en el mismo momento y medio en el que se recojan los datos y remitir a información adicional y detallada disponible en un segundo nivel. • **Notificar**: comunicar el tratamiento a los interesados, cuando los datos no se recaben directamente de ellos, en momento en que estos hayan sido obtenidos y a más tardar en el plazo de un mes, o si van a utilizarse	

Tabla 5. Privacidad desde el diseño			
Estrategia	**Objetivo**	**Controles de privacidad**	**Ejemplos**
		para comunicarse con ellos, en la primera comunicación. También se les debe comunicar si está previsto transferir los datos a terceras partes. Igualmente deben implementarse mecanismos para notificar a los interesados las violaciones de seguridad que hayan ocurrido y que puedan suponer un alto riesgo para sus derechos y libertades, utilizando un lenguaje claro y sencillo en el que se describa la naturaleza de la vulneración.	
Controlar	Proporcionar a los titulares control en relación a la obtención, tratamiento, usos y comunicaciones realizadas sobre sus datos personales mediante la implementación de mecanismos que permitan el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad así como la prestación y retirada del consentimiento o la modificación de las opciones de privacidad en aplicaciones y servicios.	• **Consentir**: recoger el consentimiento de los sujetos de datos, en aquellos casos en los que no haya otra base de legitimación, y que debe ser prestado de manera inequívoca, mediante manifestación o una clara acción afirmativa, debiendo ser explícito en determinadas situaciones como el tratamiento de datos sensibles, la adopción de ciertas decisiones automatizadas o las transferencias internacionales. Además, el titular debe poder retirar su consentimiento en cualquier momento, mediante mecanismos y procedimientos que garanticen que es tan fácil retirarlo como prestarlo. • **Alertar**: hacer al usuario consciente del momento en el que se está realizando la	• Paneles de preferencias de privacidad • Transmisión activa de presencia • Selección de credenciales • Consentimiento informado

Tabla 5. Privacidad desde el diseño			
Estrategia	**Objetivo**	**Controles de privacidad**	**Ejemplos**
		obtención de datos personales aun cuando ya haya sido informado de manera genérica de la base legal que justifica el tratamiento o incluso este haya prestado su consentimiento. • **Elegir**: proporcionar la funcionalidad granulada[42] de aplicaciones y servicios, en particular la funcionalidad básica, sin que esta esté supeditada al consentimiento del tratamiento de datos personales que no sean necesarios para su ejecución. • **Actualizar**: implementar mecanismos que faciliten a los titulares o incluso les permita realizar directamente, en aquellos casos que sea posible, la revisión, actualización y rectificación de los datos que se hayan facilitado para un tratamiento concreto de manera que sean exactos y se ajusten a la realidad. • **Retirar**: proporcionar mecanismos para que los titulares puedan suprimir o solicitar el borrado de los datos personales que hayan facilitado a un responsable en el marco de un tratamiento.	
Cumplir	Asegurar que los tratamientos de datos personales son	• **Definir**: especificar una política de protección de datos que sea el reflejo	• Evaluación de impacto de privacidad en

[42] Las funcionalidades que requieran una legitimación basada en el consentimiento han de poderse seleccionarse de forma independiente tanto del propósito principal del objeto como entre ellas.

Tabla 5. Privacidad desde el diseño			
Estrategia	**Objetivo**	**Controles de privacidad**	**Ejemplos**
	compatibles y respetan los requisitos y obligaciones legales impuestos por la normativa.	interno de los avisos de privacidad comunicadas a los titulares. Deben crearse las estructuras y asignarse los recursos necesarios para dar soporte a esta política y que garanticen que las actividades de tratamiento llevadas a cabo por la organización respetan y son conformes a la normativa en materia de protección de datos. También debe elaborarse y llevarse a cabo un plan de formación y concienciación para todos los miembros de esta que busque garantizar una actitud comprometida y responsable como parte de la responsabilidad proactiva. • **Mantener**: dar soporte a la política definida mediante el establecimiento de procedimientos y la implantación de las medidas técnicas y administrativas necesarias. Debe revisarse la existencia de mecanismos y procedimientos efectivos para garantizar el ejercicio de derechos, la gestión y notificación de incidentes de seguridad, la adecuación de los posibles encargos de tratamiento a los requisitos legales y la acreditación del cumplimiento de las obligaciones impuestas por la normativa. • **Defender**: asegurar el cumplimiento, eficacia y eficiencia de la política de privacidad y de los procedimientos, medidas y controles implantados para	soluciones de gestión de identidad federada • Control de acceso • Gestión de obligaciones • Políticas adheridas

Tabla 5. Privacidad desde el diseño			
Estrategia	**Objetivo**	**Controles de privacidad**	**Ejemplos**
		verificar que responden en todo momento a la realizad de las actividades de tratamiento y al día a día de la organización.	
Demostrar	Demostrar, tanto a los titulares como al órgano garante, el cumplimiento de la política de protección de datos que esté aplicando, así como del resto de requisitos y obligaciones legales impuestos por la normativa en la materia.	• **Registrar**: documentar todas y cada una de las decisiones tomadas en el tiempo aun cuando hayan resultado contradictorias, identificando quién las tomó, cuándo y la justificación para hacerlo. • **Auditar**: revisar de forma sistemática, independiente y documentada el grado de cumplimiento de la protección de datos. • **Informar**: documentar los resultados de las auditorías realizadas y cualquier incidente que se produzca en las operaciones de tratamiento de datos personales y ponerlo a disposición del órgano garante cuando sea necesario. En el caso de nuevos tratamientos y si el resultado de la evaluación de impacto relativa a la protección de datos arroja que el tratamiento entrañaría un alto riesgo para los derechos y libertades de los interesados si el responsable no toma medidas para mitigarlos, realizar la consulta previa al INAI.	• Auditoría • Registro

Protección de datos por defecto hace referencia a las elecciones realizadas con respecto a los valores de configuración u opciones de tratamiento fijadas en los sistemas y procedimientos que implementan el tratamiento y que determinan la cantidad de los datos personales recopilados, el alcance de su procesamiento, el período de su conservación y su accesibilidad.[43]

La Tabla 6 contiene el detalle de la configuración por defecto que garantiza un tratamiento respetuoso con los principios y deberes, abogando por un procesamiento mínimamente intrusivo: mínima cantidad de datos personales, mínima extensión del tratamiento, mínimo plazo de conservación, y mínima accesibilidad a datos personales, todo ello sin la intervención del titular para garantizar que se encuentran establecidos.

Tabla 6. Privacidad por defecto

Estrategia	Objetivo	Control de privacidad
Cantidad de datos personales recogidos	Considerar el volumen de datos personales tratados, el nivel de detalle, las diferentes categorías, la sensibilidad (categorías especiales de datos) y los tipos de datos personales requeridos y necesarios para llevar a cabo una operación de tratamiento, incluyendo tanto los datos recogidos como los generados o inferidos a partir de estos.	• **Evitación de datos**: Se evitará todo tratamiento de datos personales cuando ello sea posible para cumplir la finalidad pertinente. • **Limitación**: Se limitará la cantidad de datos personales recogidos a lo estrictamente necesario para el fin previsto. • **Limitación de acceso**: Se configurará el tratamiento de datos de manera que se minimice el número de personas que necesiten acceder a datos personales para desempeñar sus funciones, y se limitará el acceso en consecuencia. • **Pertinencia**: Los datos personales deben ser pertinentes para el tratamiento en cuestión, y el responsable del tratamiento deberá poder acreditar dicha pertinencia. • **Necesidad**: Cada categoría de datos personales será necesaria para los fines especificados y solo deberá ser objeto de tratamiento si no es posible cumplir la finalidad por otros medios.

[43] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default"

Tabla 6. Privacidad por defecto		
Estrategia	**Objetivo**	**Control de privacidad**
		• **Agregación**: Deberán utilizarse datos agregados cuando sea posible. • **Seudonimización**: Se deberán seudonimizar los datos personales en cuanto ya no sea necesario tener datos personales identificables directamente, y se conservarán las claves de identificación por separado. • **Anonimización y supresión**: Cuando los datos personales no sean o hayan dejado de ser necesarios para el fin previsto, serán anonimizados o suprimidos. • **Flujo de datos**: El flujo de datos deberá ser lo suficientemente eficiente como para no crear más copias de las necesarias. • **Estado de la técnica**: El responsable del tratamiento debe aplicar tecnologías actualizadas y adecuadas para evitar y minimizar el uso de datos.
Extensión del tratamiento	Limitar las operaciones de tratamiento sobre los datos personales realizadas por el responsable a lo estrictamente necesario para cumplir con el propósito declarado.	• Las operaciones que se realizan en cada una de las fases del ciclo de vida del dato deben ser únicamente las necesarias, y sobre los datos necesarios, para el cumplimiento de la finalidad de dicha fase, en particular en función de los casos de uso.
Periodo de conservación	Limitar al periodo de conservación vinculado con la extensión del tratamiento ya que la conservación de los datos es, en sí, una operación de tratamiento. La aplicación del principio de minimización sobre el periodo de conservación establece que, si un dato personal no se necesita más después de ejecutar una fase del tratamiento, el dato deberá ser suprimido (lo que podría suponer en algunos casos el bloqueo o la	• **Supresión y anonimización**: El responsable del tratamiento debe tener procedimientos y funcionalidades claros de supresión y anonimización. • **Eficacia de la anonimización o supresión**: El responsable del tratamiento se asegurará de que no sea posible volver a identificar los datos anonimizados o recuperar

Tabla 6. Privacidad por defecto		
Estrategia	**Objetivo**	**Control de privacidad**
	anonimización). Cualquier retención deberá ser objetivamente justificable y fundamentada.	datos suprimidos, y deberá comprobar si esto es posible. • **Automatización**: La supresión de determinados datos personales debe ser automatizada. • **Criterios de conservación:** El responsable del tratamiento debe determinar qué datos y qué plazos de conservación son necesarios para los fines previstos. • **Justificación**: El responsable del tratamiento deberá poder justificar por qué el plazo de conservación es necesario para los fines y los datos personales en cuestión, así como explicar el razonamiento y los fundamentos jurídicos del plazo de conservación. • **Ejecución de las políticas de conservación:** El responsable del tratamiento debe aplicar políticas internas de conservación y realizar pruebas para determinar si la organización pone en práctica sus políticas. • **Copias de seguridad y registros**: Los responsables del tratamiento deben determinar qué datos personales y plazos de conservación son necesarios para las copias de seguridad y los registros. • **Flujo de datos**: Los responsables del tratamiento deben ser cuidadosos con el flujo de datos personales y la conservación de sus copias, y procurar limitar su conservación temporal.
Accesibilidad de los datos	Establecer quién puede acceder a los datos personales, tanto en lo que respecta al personal dentro de la organización como a terceros, ya sean otras entidades y organismos o incluso sistemas automatizados	Este análisis se deberá realizar para cada una de las fases del tratamiento y se implementará mediante:

Tabla 6. Privacidad por defecto		
Estrategia	**Objetivo**	**Control de privacidad**
	como motores de búsqueda, servidores en la nube, o cualquier otro sistema aplicación o servicio que acceda a los datos utilizados en el tratamiento.	• Una definición de roles y responsabilidades de los miembros de la organización. • Una política de control de privilegios de acceso como parte de las medidas administrativas adoptadas. • La incorporación de mecanismos de control de acceso a la información que implementen la política definida y que serán en parte de carácter administrativo y de tipo técnico.
Documentación y auditoría	Documentar y recoger la información suficiente para permitir, de forma satisfactoria y demostrable, acreditar el cumplimiento de la normativa en la materia	• Comprobar que está disponible en la entidad responsable la documentación necesaria para: la definición de roles y obligaciones de los miembros de la organización, la política de control de accesos, la política de información y cualquier otra documentación significativa. • Comprobar que la entidad tiene implementados procedimientos que garanticen el cumplimiento de las políticas anteriores y que están operativos. • Comprobar que está disponible la información básica relativa al tratamiento, en particular, sobre la naturaleza, el ámbito, el contexto y los fines, así como el análisis de proporcionalidad y necesidad. • Tener documentado un análisis del tratamiento por fases del ciclo de vida de los datos personales e identificar para cada fase las operaciones, la implementación organizativa y técnica, los datos personales y los intervinientes internos y externos, las interacciones, servicios, sistemas y operaciones compartidos con otros tratamientos

Tabla 6. Privacidad por defecto		
Estrategia	**Objetivo**	**Control de privacidad**
		• Comprobar que el ciclo de vida de los datos está ajustado a los casos de uso • Comprobar que el responsable no obliga al usuario a aceptar un tratamiento más intrusivo (mayor cantidad de datos o una mayor extensión en las operaciones) como condición para acceder a un servicio

FASE 7. RESULTADOS DE LA O LAS CONSULTAS EXTERNAS QUE, EN SU CASO, SE EFECTÚEN

De manera previa a la presentación de la EIPD ante el INAI, el área responsable, con apoyo de la Unidad de Transparencia, podrá llevar a cabo consultas externas con los titulares o público involucrado en la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que pretenda implementar o modificar y que implique un tratamiento intensivo o relevante de datos personales.[44]

En caso de realizar alguna consulta, el área responsable deberá informar[45] sobre su resultado señalando:

a) las opiniones, puntos de vista y perspectivas del público que, a su juicio, consideró pertinente incorporar en el diseño o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales,

b) las opiniones que no consideró, especificando las razones o motivos que lo llevaron a tal decisión.

La Unidad de Transparencia documentará el resultado de esta fase en el Informe de EIPD, incluyendo los documentos recabados de la consulta.

[44] Artículo 13 de las Disposiciones Administrativas.

[45] Artículo 21 de las Disposiciones Administrativas.

En caso de no haber realizado una consulta externa, la Unidad de Transparencia señalará la inexistencia con la siguiente leyenda:

> "No se actualiza el supuesto debido a que el INE no consideró necesaria la ejecución de consultas públicas, de acuerdo con los señalado en el artículo 13 de las Disposiciones administrativas."

FASE 8. OPINIÓN TÉCNICA DEL OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

Si bien, las Disposiciones administrativas señalan que se debe integrar la opinión técnica del Oficial de Protección de Datos Personales[46], este supuesto no se actualiza debido a que, de conformidad con el artículo 58 del Reglamento del Instituto Nacional Electoral en materia de protección de datos personales, la Unidad de Transparencia es la responsable de realizar la evaluación de impacto, en los casos previstos en la Ley General -junto con el área responsable del tratamiento-.

La Unidad de Transparencia señalará la inexistencia con la siguiente leyenda, en tanto esta condición no cambie en el Instituto:

> "No se actualiza el supuesto debido a que:
>
> a) La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece como optativo contar con un Oficial de Protección de Datos Personales, el Instituto Nacional Electoral actualmente no dispone de esta figura.
>
> b) La Unidad de Transparencia es la responsable de realizar la evaluación de impacto, en los casos previstos en la Ley General -junto con el Órgano responsable del tratamiento-, de conformidad con el artículo 58 del Reglamento del Instituto Nacional Electoral en materia de protección de datos personales."

En caso de un cambio en este supuesto, la Unidad de Transparencia integrará la opinión correspondiente.

La Unidad de Transparencia documentará el resultado de esta fase en el Informe de EIPD.

FASE 9. CUALQUIER OTRA INFORMACIÓN O DOCUMENTOS QUE CONSIDERE CONVENIENTE HACER DEL CONOCIMIENTO DEL INAI

En esta fase, el área responsable deberá proveer a la Unidad de Transparencia de toda la información extra (que no haya sido integrada en apartados anteriores) que consideren

[46] Artículo 22 de las Disposiciones Administrativas.

pertinente de 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.

Ejemplo de esta información o documentos son:

- Funcionamiento del sistema;
- Normativa;
- Manuales de usuario y técnicos;
- Resultados de pruebas de seguridad (pruebas de penetración o análisis de vulnerabilidades);
- Convenios, por mencionar algunos.

La Unidad de Transparencia documentará el resultado de esta fase en el Informe de EIPD.

PARTE IV. INFORME DE EIPD Y REQUERIMIENTOS DE INFORMACIÓN

ELABORAR Y ENVIAR EL INFORME

La Unidad de Transparencia elaborará el Informe de EIPD que estará conformado por toda la información recabada y analizada de las secciones “Parte II y Parte III” de este documento.

Para su elaboración utilizará el **Formato “Informe EIPD”, disponible en el Anexo XII de este documento.**

El Informe debe ser firmado por las siguientes figuras:

- Por parte de la Unidad de Transparencia:
    - Las personas que ejecutaron la EIPD.
    - La persona a cargo de la Subdirección de Gobierno de Protección de Datos.
    - La persona a cargo de la Dirección de Acceso a la Información y protección de Datos Personales.
- Por parte del área responsable, las personas con los siguientes cargos:
    - Jefatura de Departamento.
    - Subdirección de Área.
    - Dirección de Área.

La Unidad de Transparencia enviará el Informe de EIPD al INAI, de conformidad con lo establecido en las *"Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, Capítulo IV".*

REQUERIMIENTO DE INFORMACIÓN

En caso de que el INAI considere que requiere más elementos para el análisis de la evaluación de impacto, el área responsable con apoyo de la Unidad de Transparencia, atenderán el requerimiento, de conformidad con lo establecido en las "Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, Capítulo IV".

ANEXOS

Los formatos y documentos a que hace referencia esta metodología están disponibles en el siguiente repositorio.

Num.	Formato / Documento	Documento
I	Condiciones generales y adicionales	I. Condiciones generales y adicionale
II	Informe de exención EIPD	II. Informe exención.docx
III	Preparación de la EIPD	III. Preparación de la EIPD.docx
IV	Identificación de información obligatoria	IV. Identificación de información obligator
V	Identificación de información adicional	V. Identificación de información adicional
VI	Justificación de la necesidad	VI. Justificación de la necesidad.docx
VII	Inventario de datos personales	VII. Inventario de datos personales.7z
VIII	Criterios para elaborar el Diagrama de flujo de datos personales	VIII. Criterios para elaborar el Diagrama
IX	Modelo de Ciclo de vida de la información	IX. Modelo de Ciclo de vida de la informa
X	Metodología de Análisis de Riesgos Tomos I y II	X. Metodología Riesgos PDP.zip

Num.	Formato / Documento	Documento
XI	Análisis de cumplimiento normativo	XI. Análsis del cumplimiento normati
XII	Informe de EIPD	XII. Informe EIPD.docx

REFERENCIAS

1. Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit. European Data Protection Supervisor. April 2017.
2. Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. Agencia Española de Protección de Datos. Junio 2021.
3. Guide to Data Protection Impact Assessments. Personal Data Protection Commission Singapore, 2021.
4. Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. European Data Protection Supervisor. December 2019.
5. ISO/IEC 29134. Information technology – Security techniques – Guidelines for privacy impact assessment. First edition 2017-06.
6. WP 248 rev.01. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. Article 29 Data Protection Working Party. October 2017.