DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Cuadernos DivalData

Cuadernos dirigidos a delegados,
responsables y especialistas en protección
de datos personales

Cuaderno nº 17 | Noviembre 2021

DIRECTRICES PARA LA ELABORACIÓN DE UNA EVALUACIÓN DE IMPACTO EN PROTECCIÓN DE DATOS

Í N D I C E

DIRECTRICES PARA LA ELABORACIÓN DE UNA EVALUACIÓN DE IMPACTO EN PROTECCIÓN DE DATOS

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirte a nuestra publicación accede al siguiente

enlace

UNA EVALUACIÓN DE IMPACTO ES UN PROCESO UTILIZADO PARA REFORZAR Y DEMOSTRAR EL CUMPLIMIENTO

INTRODUCCIÓN

La gestión del riesgo es uno de los pilares de la dirección de cualquier organización. Toda entidad o corporación, cuando pretende iniciar con garantías un nuevo producto o servicio, debe gestionar los elementos de incertidumbre que se derivan de su naturaleza, ámbito, contexto y fines.

El Reglamento General de Protección de Datos hace referencia al término "riesgo" en setenta y tres ocasiones a lo largo del texto. Particularmente, el artículo 35, introduce el concepto de evaluación de impacto relativa a la protección de datos (EIPD).

En el texto del Reglamento no aparece una definición para el término "evaluación de impacto relativa a la protección de datos", pero el Comité Europeo de Protección de Datos sí desarrolla la definición de EIPD en las Directrices WP248 como "un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales evaluándolos y determinando las medidas para abordarlos."

Las EIPD son instrumentos importantes para la rendición de cuentas, ya que ayudan a los responsables no solo a cumplir los requisitos del RGPD, sino también a demostrar que se han tomado medidas adecuadas para garantizar el cumplimiento del Reglamento (vid. art. 24).

En otras palabras, una EIPD es un proceso utilizado para reforzar y demostrar el cumplimiento.

En virtud del RGPD, el incumplimiento de los requisitos de la EIPD puede dar lugar a la imposición de sanciones por parte de la Agencia Española de Protección de Datos. La sanción puede ser impuesta por:

- No llevar a cabo una EIPD cuando el tratamiento requiera una evaluación de este tipo;
- Llevar a cabo una EIPD de forma incorrecta;
- No consultar a la autoridad de control cuando sea necesario.

Analicemos estos extremos.

"LOS RESPONSABLES DE LOS TRATAMIENTOS DE DATOS DE REALIZAR UNA EIPD CON CARÁCTER PREVIO A LA PUESTA EN FUNCIONAMIENTO DE TALES TRATAMIENTOS CUANDO SEA PROBABLE QUE ÉSTOS POR SU NATURALEZA, ALCANCE, CONTEXTO O FINES ENTRAÑEN UN ALTO RIESGO PARA LOS DERECHOS Y LIBERTADES DE LAS PERSONAS FÍSICAS".

CUÁNDO DEBE REALIZARSE LA EIPD

Una EIPD marcará la forma en que debemos hacernos cargo de los riesgos de nuestros tratamientos, adoptando las medidas que resulten preceptivas para solventarlos, de forma que podamos garantizar que los datos personales sean debidamente protegidos.

Es decir, la finalidad que se persigue al realizar una EIPD es posibilitar que los responsables del tratamiento adopten medidas tendentes a reducir esos riesgos que nos obligan a hacerla (disminuyendo la probabilidad de su materialización y las consecuencias negativas para los usuarios).

El apartado 1 del artículo 35 del RGPD establece, con carácter general, la obligación que tienen los responsables de los tratamientos de datos de realizar una EIPD con carácter previo a la puesta en funcionamiento de tales tratamientos cuando sea probable que éstos por su naturaleza, alcance, contexto o fines entrañen un alto riesgo para los derechos y libertades de las personas físicas, alto riesgo que, según el propio Reglamento, se verá incrementado cuando los tratamientos se realicen utilizando "nuevas tecnologías".

El artículo 35.3 establece que la EIPD se requerirá en particular en uno de estos casos:

- evaluación sistemática y exhaustiva de aspectos personales de 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 las personas físicas o que les afecten significativamente de modo similar;
- tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 del RGPD;
- observación sistemática a gran escala de una zona de acceso público.

UN PRIMER ANÁLISIS CUALITATIVO PUEDE CONCLUIR QUE NO ES NECESARIO REALIZAR DICHA EIPD, PERO HAY QUE JUSTIFICARLO

Para facilitar a los responsables de los tratamientos la identificación de aquellos tratamientos que no requieren una EIPD, el RGPD dispone que las autoridades de control podrán –como hace nuestra AEPD– publicar listas con los tratamientos que requieren y no requieran de la elaboración de una EIPD. Dichas listas están enlazadas en el apartado de Material complementario, pero veamos algunos ejemplos.

EJEMPLOS DE SUPUESTOS OBLIGATORIOS

- Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos.
- Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.
- Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.
- Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.

CATEGORÍAS ESPECIALES DE DATOS,TRATAMIENTOS A GRAN ESCALA O EMPLEO DE LAS NUEVAS TECNOLOGÍAS PUEDEN MOTIVAR LA NECESIDAD DE UNA EIPD

- Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.
- Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.
- Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos
- Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 "Directrices sobre los delegados de protección de datos (DPD)" del Grupo de Trabajo del Artículo 29.
- Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.
- Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b,c,d) del RGPD.

EXENCIÓN DE LA OBLIGACIÓN

¿Están considerando un nuevo tratamiento y no saben si requeriría realizar una evaluación de impacto?

La AEPD publicita ejemplos de tratamientos exentos de realizar una EIPD:

NUEVOS TRATAMIENTOS QUE SEAN NECESARIOS PARA EL CUMPLIMIENTO DE UNA OBLIGACIÓN LEGAL, CUMPLIMIENTO DE UNA MISIÓN REALIZADA EN INTERÉS PÚBLICO O EN EL EJERCICIO DE PODERES PÚBLICOS CONFERIDOS AL RESPONSABLE PODRÍAN ESTAR EXENTOS

- Tratamientos que se realizan estrictamente bajo las directrices establecidas o autorizadas con anterioridad mediante circulares o decisiones emitidas por las Autoridades de Control, en particular la AEPD, siempre y cuando el tratamiento no se haya modificado desde que fue autorizado.
- Tratamientos que se realizan estrictamente bajo las directrices de códigos de conducta aprobados por la Comisión Europea o las Autoridades de Control, en particular la AEPD, siempre y cuando una EIPD completa haya sido realizada para la validación del código de conducta y el tratamiento se implementa incluyendo las medidas y salvaguardas definidas en la EIPD.
- Tratamientos que sean necesarios para el cumplimiento de una obligación legal, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, siempre que en el mismo mandato legal no se obligue a realizar una EIPD, y siempre y cuando ya se haya realizado una EIPD completa.
- Tratamientos realizados en el ejercicio de su labor profesional por trabajadores autónomos que ejerzan de forma individual, en particular médicos, profesionales de la salud o abogados, sin perjuicio de que pueda requerirse cuando el tratamiento que lleven a cabo cumpla, de forma significativa, con dos o más criterios establecidos en la lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos publicada por la AEPD.
- Tratamientos obligatorios por ley y realizados con relación a la gestión interna del personal de las PYMES con finalidad de contabilidad, gestión de recursos humanos y nóminas, seguridad social y salud laboral, pero nunca relativos a los datos de los clientes.

También se mencionan algunos supuestos relativos a comunidades de propietarios y colegios profesionales y asociaciones sin ánimo de lucro.

HAY QUE EMPEZAR POR DESCRIPCIÓN SISTEMÁTICA DE LAS OPERACIONES DE TRATAMIENTO PREVISTAS Y DE LOS FINES DEL TRATAMIENTO, INCLUSIVE, CUANDO PROCEDA, EL INTERÉS LEGÍTIMO PERSEGUIDO POR EL RESPONSABLE DEL TRATAMIENTO

EIPD = GESTIÓN DE RIESGOS

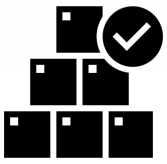
Cabe recordar que estamos ante el proceso de identificar, evaluar y gestionar los riesgos.

Nuestro estudio deberá incluir, pues, una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento; una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; y una evaluación de los riesgos para los derechos y libertades de los interesados.

En otras palabras, esta gestión de riesgos se divide en tres partes:

La **identificación de las amenazas** (factores de riesgo concurrentes que, en caso de materializarse, puede provocar daños a los derechos de los interesados) **y de los riesgos** (la combinación de la posibilidad de que se materialicen las amenazas previamente identificadas y sus consecuencias).

La **evaluación de los riesgos** (consiste en valorar el impacto (significativo o no) de la exposición a la amenaza, entendido como los posibles daños que se pueden producir si la amenaza se materializa, junto a la probabilidad de que esta se materialice).



El **tratamiento de los riesgos** detectados. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

EL RESPONSABLE DEL TRATAMIENTO ES QUIEN REALIZARÁ LA EIPD, CON ASESORAMIENTO DEL DELEGADO DE PROTECCIÓN DE DATOS (POR SU FUNCIÓN DE APOYO Y ASESORAMIENTO)

CÓMO ABORDAR UNA EIPD

El responsable del tratamiento es quien realizará la EIPD, con asesoramiento del Delegado de Protección de Datos (por su función de apoyo y asesoramiento), si hubiera sido nombrado, o del encargado del tratamiento, según lo dispuesto en contrato de encargo del tratamiento, en su caso.

Asimismo, podrían concurrir otras personas o figuras, con diferentes roles y responsabilidades. Si procede, el responsable recabará la opinión de los interesados en relación con el tratamiento previstos.

Para la metodología, existen indicaciones de la AEPD y un modelo a los efectos de poder utilizarse en las administraciones públicas (véase el apartado de material complementario).

En esencia, la evaluación debe incluir las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el Reglamento.

El contenido de la evaluación deberá incluir como mínimo:

1. Una exposición ordenada de las actividades de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento. *Véase el Anexo I de la Guía AEPD para la realización de EIPD.*
2. Una valoración de la exigencia y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad. *Anexo II de la Guía AEPD para realizar EIPD.*
3. Una apreciación de los peligros para los derechos y libertades de los interesados.
4. Las medidas contempladas para hacer frente a los riesgos y amenazas.
5. Garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de datos personales y a demostrar la conformidad con el reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

LOS RIESGOS QUE HEMOS DE OBSERVAR SON TANTO AQUELLOS RELATIVOS A LAS PERSONAS, COMO LOS QUE PUEDEN AFECTAR A LA ORGANIZACIÓN SI NO CUMPLIMOS CON LA PROTECCIÓN DE DATOS

FASES

- IDENTIFICAR LA NECESIDAD DE UNA EIPD

Como ya se indicó, realizar un EIPD no es una obligación para todas las organizaciones, aunque es recomendable hacerlo en todos los casos que se traten datos personales. Cuando no sea obligatorio se puede optar por una aproximación menos formalizada. El resultado ayudará a a proteger los datos, mantener una buena reputación y evitar sanciones.

- ANÁLISIS DEL PROYECTO Y FLUJOS DE INFORMACIÓN

Esta segunda etapa es de gran importancia para realizar una buena EIPD. Para ello, será necesario analizar en profundidad el proyecto que engloba el tratamiento de datos personales, como por ejemplo categorías tratadas, actores implicados, tecnologías, cesiones a terceros, etc.

- IDENTIFICACIÓN RIESGOS

Con toda la información obtenida en la etapa anterior se deberán identificar los posibles riesgos a los que están expuestos los datos, valorar la probabilidad y el impacto que tendría la materialización de la amenaza.

Los riesgos pueden ser de dos tipos:

- Para las personas, el principal a tener en cuenta, puede poner en riesgo su privacidad;
- Para la organización, cuando no implementase una correcta política de protección de datos.

- GESTIÓN DE RIESGOS

Una vez analizado el proyecto y definidos los riesgos, se deberán identificar los controles y medidas de seguridad necesarias. Esta fase debe ser llevada a cabo y consensuada entre todos los actores implicados en el tratamiento.

- CUMPLIMIENTO NORMATIVO

Se comprobará que el contenido de la EIPD cumple con la legislación en materia de protección de datos (LOPDGDD y RGPD), así como, en su caso, la demás legislación aplicable por ser de obligado cumplimiento.

SE DEBERÁN APLICAR LAS MEDIDAS NECESARIAS PARA PROTEGER LOS DATOS PERSONALES INDICADAS POR LOS RESPONSABLES DE LA ENTIDAD O CORPORACIÓN

- INFORME FINAL

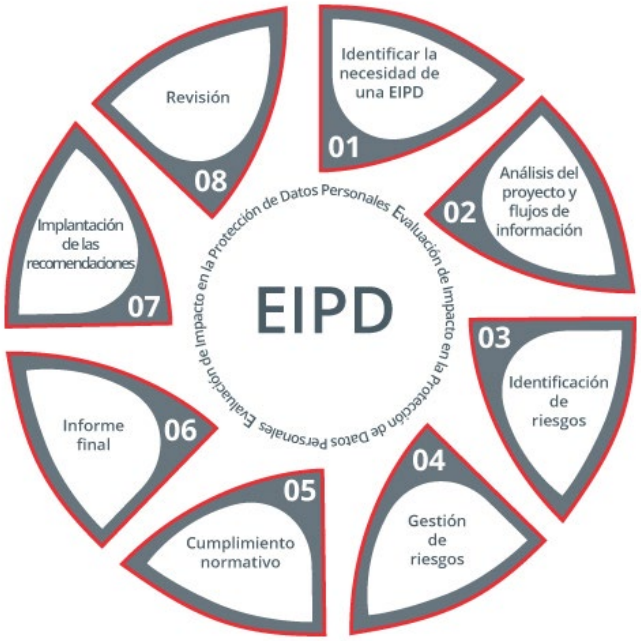
En el informe final se incluirá toda la información que se ha generado durante las etapas anteriores. Este informe deberá estar elaborado con un lenguaje claro, evitando la inclusión de tecnicismos de cualquier tipo. Dicho informe será remitido a los máximos responsables de la organización para que tomen las decisiones necesarias en función de las recomendaciones indicadas.

- IMPLANTACIÓN DE LAS RECOMENDACIONES

Una vez revisado el informe, se deberán aplicar las medidas necesarias para proteger los datos personales indicadas por los responsables de la organización. En esta fase se definirán los recursos necesarios y el responsable de su ejecución.

- REVISIÓN

Una vez terminado el proceso se analizará el resultado final y la efectividad de los controles tomados. También se identificarán nuevos riesgos a los que están expuestos los datos.



Fuente: INCIBE

MATERIAL COMPLEMENTARIO

- "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales" (guía de la AEPD). Consulta en este enlace.
- Lista de tratamientos que requieren evaluación de impacto relativa a protección de datos (AEPD). Consulta en este enlace.
- Lista orientativa de tipos de tratamientos de datos que no requieren una evaluación de impacto relativa a la protección de datos (AEPD). Consulta en este enlace.
- Herramienta "Evalúa-Riesgo RGPD" (AEPD). Consulta en este enlace.
- Herramienta "Gestiona EIPD" (AEPD). Consulta en este enlace.

NOTICIAS

- **La AEPD publica un modelo de informe para ayudar a las empresas a realizar evaluaciones impacto en la protección de datos.**

  El documento recopila los aspectos que deben ser tenidos en cuenta por el sector privado para elaborar un informe de Evaluación de Impacto (EIPD), complementando a la Guía práctica publicada por la Agencia. Consulta la publicación en este enlace.

- **El BOE publica la Instrucción 1/2021, de 2 de noviembre, de la Agencia Española de Protección de Datos, por la que se establecen directrices respecto de la función consultiva de la Agencia, de conformidad con el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de esos datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y el Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio.**

  La instrucción será de aplicación a la actividad consultiva de la AEPD. Consulta la Instrucción en este enlace.

- **La Agencia Española de Protección de Datos (AEPD) ha sancionado al Ayuntamiento de Molina de Segura por carecer de delegado de protección de datos.**

  Consulta la noticia en este enlace.