Análisis de riesgos y evaluación de impacto relativa a la protección de datos: su aplicación a las sociedades cooperativas

(Risk analysis and impact assessment relating to data protection: its application to cooperative companies)

Enrique Gadea Soler[1]
Universidad de Deusto (España)

doi: http://dx.doi.org/10.18543/baidc-56-2020pp47-72

Recibido: 25.07.2019
Aceptado: 21.02.2020

[1] Profesor Titular de Derecho Mercantil de la Universidad de Deusto. Email: egadea@deusto.es

Resumen: El RGPD impone a todas las empresas realizar un análisis de riesgo en los tratamientos de datos personales. Si este análisis indica que existe un alto riesgo será obligatorio realizar una EIPD, con el objeto de prever los impactos y riesgos que los mismos pueden suponer en la privacidad de los interesados. De ese modo, y sobre esa base, el RGPD exige que se implanten las medidas de seguridad y control para garantizar los derechos y libertades de las personas. Este trabajo se centra, por una parte, en analizar cuándo una sociedad cooperativa debe realizar una EIPD y, por otra, en estudiar cuales son las fases que debe comprender la realización de una correcta EIPD.

Palabras clave: Evaluación de impacto en la protección de datos y sociedades cooperativas.

Abstract: The GDPR requires all businesses to conduct a risk analysis of the processing of personal data. If this analysis shows that there is a high risk, it will be mandatory to perform a DPIA in order to foresee the impacts and risks this may pose to the privacy of the interested parties. On this basis, the GDPR requires the implementation of security and control measures to guarantee the rights and freedoms of individuals. This paper focuses, on the one hand, on analysing when a cooperative society must carry out a DPIA and, on the other hand, on studying the phases involved in conducting a DPIA correctly.

Keywords: Data protection impact assessment and cooperative societies.

I. **Introducción**

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 a la libre circulación de estos datos (en lo sucesivo, indistintamente, Reglamento General de Protección de Datos o RGPD) es de aplicación obligatoria desde el 25 de mayo de 2018 para todas las organizaciones, empresas, autónomos y administraciones que traten información sobre una persona física identificada o identificable, y, por tanto, también a las sociedades cooperativas (Un comentario sobre el mismo, puede verse en: LÓPEZ CALVO, 2017, 27 y ss.). El RGPD ha sido desarrollado y complementado en el ámbito interno por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (o, indistintamente, LOPDGDD).

Una de las novedades de la nueva regulación es la obligación que se impone a todas las empresas de realizar un análisis de riesgo de los tratamientos iniciados antes del 25 de mayo de 2018. Si este análisis indica que existe un alto riesgo, será obligatorio realizar una Evaluación de Impacto en la Protección de Datos Personales (o, indistintamente, EIPD. También conocida como PIA: Privacy Impact Assement) y adoptar las cautelas correspondientes para cumplir con las exigencias del Reglamento Europeo y de la normativa interna en materia de protección de datos, con las que se pretende que se implanten las medidas de seguridad y control para garantizar los derechos y libertades de las personas.

El objetivo de este trabajo se centra, por una parte, en analizar cuándo se debe realizar una EIPD, por no ser suficiente con un análisis básico de riesgos, y, por otra, de ser necesaria, cuales son las fases que debe comprender la EIPD.

No debe olvidarse que cualquier actividad económica lícita podrá ser organizada y desarrollada mediante una sociedad cooperativa. En ese sentido, cabe señalar a priori que las entidades que tienen que realizar una evaluación de impacto relativa a la protección de datos son aquellas que se dedican a actividades relacionadas con el sector asegurador, financiero y crediticio, farmacéutico, hospitales y clínicas, seguridad privada, vigilancia y control, comercializadores de energía, empresas que realizan e-comerce o colegios.

II. **Concepto y finalidad de una evaluación de impacto en la protección de datos**

La Evaluación de Impacto en la Protección de Datos Personales es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos. El análisis de riesgos para un determinado tratamiento permite identificar los riesgos que se ciernen sobre los datos de los interesados y establecer una respuesta adoptando las salvaguardas necesarias para reducirlos hasta un nivel de riesgo aceptable.

Por tanto, una Evaluación de Impacto consiste en una identificación y evaluación de los potenciales riesgos y efectos que, en los aspectos y requerimientos de privacidad, podrían tener nuevos servicios, operaciones, procesos, proyectos, programas, iniciativas, políticas, sistemas, productos o tecnologías, dado que implican tratamientos de datos personales y produce como resultado una respuesta sobre si se aceptan, mitigan o evitan dichos riesgos, identificando las soluciones o medios correspondientes.

El objetivo es, por un lado, conseguir una protección más activa del derecho fundamental a la protección de datos y, por otro, potenciar las políticas preventivas entre las organizaciones para evitar tanto costosos rediseños de los sistemas una vez han sido desarrollados, como posibles daños a la reputación y la imagen por un tratamiento inadecuado de los datos personales (PUYOL, 2018, 9).

La Evaluación de Impacto en materia de protección de datos no es una lista de verificación de cumplimiento, sino que viene a constituir una auténtica «herramienta» esencial para conseguir una eficaz evaluación de los riesgos que, para la privacidad de las personas, tiene cualquier sistema que trate datos de carácter personal (RECIO GAYO, 2016, 132).

No obstante, a pesar de lo mencionado anteriormente, no hay obstáculo para plantear una EIPD para tratamientos que ya estén en plena explotación (MUÑOZ DEIROS, 2014).

Como muy acertadamente ha destacado el Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales del artículo 29 (en adelante, GT 29) en su guía (WP248 Guías sobre las Evaluaciones de Impacto en Protección de Datos): «*una Evaluación de Impacto es 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».*

Boletín de la Asociación Internacional de Derecho Cooperativo
ISSN: 1134-993X • ISSN-e: 2386-4893, No. 56/2020, Bilbao, págs. 47-72
doi: http://dx.doi.org/10.18543/baidc-56-2020pp47-72 • http://www.baidc.deusto.es

El RGPD entró en vigor el 24 mayo de 2016 y es de plena aplicación desde el 25 de mayo de 2018. Durante este periodo de dos años, los responsables y encargados de tratamientos han debido adecuar las operaciones de tratamiento que llevan a cabo a lo que prevé el RGPD, adoptando las medidas necesarias para atender adecuadamente las modificaciones que introduce el Reglamento y, en especial, los nuevos principios, los nuevos derechos y las nuevas obligaciones que prevé. En esa línea, entendemos que el resultado de la EIPD debe constituir un elemento clave a la hora de tomar las decisiones relacionadas con el cumplimiento de lo que prevé el RGPD (NIETO MARTÍN, 2016, 62).

Y ello porque la EIPD es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable (LÓPEZ CALVO, 2017, 52).

Las EIPD son también 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 (artículo 24 RGPD). En palabras del GT 29, una EIPD es un proceso utilizado para reforzar y demostrar el cumplimiento.

El RGPD ha reconocido en sus considerandos número 89 a 91 que la medida de inscribir los ficheros o bases de datos en el Registro General del Regulador correspondiente no ha contribuido a mejorar la protección de datos personales, y la ha sustituido por la obligación de realizar una Evaluación de Impacto, cuando sea probable que el tratamiento entrañe un alto riesgo para los derechos y libertades de los interesados o personas afectadas por dicho tratamiento**.**

La EIPD tiene que ser un proceso sistemático que se debe hacer aplicando metodologías o métodos de ejecución objetivos, repetibles y comparables; en consecuencia, la ejecución de la EIPD se tiene que estructurar en diferentes fases o etapas.

La regulación material de las Evaluaciones de Impacto se encuentra en el artículo 35 del RGPD, que, por una parte, aclara, en el apartado 1.º del artículo 35 del RGPD, párrafo in fine, que:

«*Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares*». *Y, por otra,* determina en el apartado 7.º, que: «*La evaluación deberá incluir como mínimo:*

a) 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;
b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas».

III. **Fases de una evaluación de impacto en la protección de datos**

Al realizar una EIPD es necesario disponer de un proceso sistemático a través de una metodología o procedimiento estandarizado de trabajo que permita establecer criterios comunes para garantizar la homogeneidad, repetitividad y comparabilidad en la ejecución de la EIPD. Es conveniente que la metodología seguida se ajuste a lo propugnado por la Agencia Española de Protección de Datos en su «*Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD*», de 2018, a lo requerido por el Grupo «*Protección de Datos*» del Artículo 29 (UE) en su documento «*Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento entraña probablemente un alto riesgo a efectos del Reglamento (UE) 2016/679)*», de 4 de abril de 2017, a lo pautado en la «*Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento*» de la Agencia Española de Protección de Datos, publicada en el año 2017, así como a los estándares internacionales privados de análisis de riesgos. Sobre la base de esas directrices, para abordar el contenido descrito en el artículo 35.7 del RGPD, vamos a distinguir las fases que detallamos a continuación:

1. *Análisis de la necesidad de la evaluación*

Realizar una Evaluación de Impacto en materia de Protección de Datos es prever desde el diseño de un determinado producto, servicio o sistema de información, y los tratamientos de datos personales que

Boletín de la Asociación Internacional de Derecho Cooperativo
ISSN: 1134-993X • ISSN-e: 2386-4893, No. 56/2020, Bilbao, págs. 47-72
doi: http://dx.doi.org/10.18543/baidc-56-2020pp47-72 • http://www.baidc.deusto.es

vayan a efectuarse, los impactos y riesgos que los mismos pueden suponer en la privacidad de los interesados.

Para ello, se trata de realizar un análisis de los riesgos derivados de los citados sistemas de información, productos o servicios, en relación con la privacidad de los interesados cuyos datos personales son tratados, y el impacto que dichos tratamientos tienen en relación con el cumplimiento de la normativa sobre protección de datos personales por parte de la entidad, así como los riesgos que suponen para esta en términos económicos, reputacionales, etc.

Sin embargo, lo primero que hay que valorar es la procedencia de la realización de la Evaluación de Impacto. En este sentido, la Agencia Española de Protección de Datos (o, indistintamente, AEPD) ha señalado que la realización de una Evaluación de Impacto en materia de Protección de Datos, cobra especial importancia en los casos en que se prevea la realización de tratamientos de datos personales que tenga como finalidad la satisfacción de alguno de los siguientes objetos, que se enuncian seguidamente:

a) El enriquecimiento de datos, mediante la recogida de nuevas categorías de datos, o se usen las existentes con nuevas finalidades, o en formas que antes no se usaban, en particular, si los nuevos usos o finalidades son más intrusivos o inesperados para los afectados.
b) El tratamiento de datos de menores de edad, sobre todo si estos son menores de 14 años.
c) El tratamiento destinado a la evaluación o predicción de aspectos personales relevantes.
d) La monitorización del comportamiento de las personas, por ejemplo, a través del análisis de la navegación por Internet.
e) Cuando se vayan a tomar decisiones que afecten a determinados colectivos, y que puedan suponer, por ello, algún tipo de discriminación.
f) Cuando se vayan a utilizar tecnologías especialmente invasivas con la privacidad. A título de ejemplo se pueden citar las siguientes: (i) la video-vigilancia a gran escala; (ii) la biometría; (iii) las técnicas genéticas; (iv) las etiquetas de radiofrecuencia o RFID; (v) la utilización de drones o aeronaves no tripuladas; (vi) la vigilancia electrónica; (vii) la minería de datos; (viii) las técnicas genéticas; (ix) la geolocalización; (x) o cualquier otra técnica de carácter análogo a las anteriores.
g) Cuando el tratamiento afecte a un número elevado de personas, y/o se produzca una acumulación de gran cantidad de da-

tos, tales como: (i) big data; (ii) internet de las cosas; o, (iii) la construcción y el desarrollo de ciudades inteligentes.

h) Cuando existan riesgos específicos de seguridad, que puedan comprometer la confidencialidad, la integridad o la disponibilidad de los datos que sean objeto de tratamiento.

i) Cuando se vayan a realizar tratamientos de datos personales en los que el responsable deje de tener el control sobre ellos, como, por ejemplo, en la contratación de servicios de Cloud Computing.

Igualmente, en el caso de prever la realización de: (i) cesiones de datos; (ii) de comunicaciones a terceros; (iii) de transferencias internacionales de datos; (iv) de tratamiento de datos especialmente sensibles; (v) de tratamientos con fines estadísticos, históricos o de investigación científica, se hace en todo caso recomendable la ejecución de un análisis de Evaluación de Impacto en materia de privacidad.

En cualquier caso, la AEPD aclara que aunque el proyecto no se ajuste a los tratamientos detallados y, por lo tanto, la entidad no parezca un candidata a ser sometida a una EIPD, hay que poner de manifiesto que siempre es una buena práctica que una organización decida llevar a cabo una evaluación de impacto en relación con tratamientos que no están entre los mencionados y asegurarse de que no le van a pasar desapercibidos posibles riesgos que, de no atajarlos, podrían tener consecuencias legales, económicas o reputacionales.

En este punto, la norma reguladora de esta cuestión que no es otra que el RGPD, prevé, en el artículo 35, apartado 1, ilustrado en el artículo 35, apartado 3, y complementado por el propio artículo 35, apartado 4, que la realización de una EIPD es obligatoria cuando el tratamiento «entrañe probablemente un alto riesgo para los derechos y libertades de las personas físicas».

En concreto, el apartado 1.º del artículo 35 del RGPD, señala que*:* «*Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares».*

A continuación, el citado apartado 1.º del artículo 35 del RGPD, antes transcrito, se concreta en el apartado 3.º de dicho precepto, que detalla los casos en los cuales se requiere la realización de la

Boletín de la Asociación Internacional de Derecho Cooperativo
ISSN: 1134-993X • ISSN-e: 2386-4893, No. 56/2020, Bilbao, págs. 47-72
doi: http://dx.doi.org/10.18543/baidc-56-2020pp47-72 • http://www.baidc.deusto.es

Evaluación de Impacto. Dichos supuestos son los que se citan a continuación:

> *«a) En la 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.*
>
> *b) En el tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1 (entre los que se encuentran los datos relativos a la salud), o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 del RGPD.*
>
> c) O, en la observación sistemática a gran escala de una zona de acceso público».

Por último, el propio artículo 35, en el apartado 4, se añade que: «*La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité (se refiere al Comité Europeo de protección de datos: CEPD) a que se refiere el artículo 68».*

En sentido similar, el artículo 28.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, establece que:

> «Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:
>
> *a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.*
>
> *b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.*
>
> *c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.*

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación».

Con el fin de garantizar una interpretación coherente de las circunstancias en las que resulta obligatoria una EIPD (artículo 35, apartado 3), recurriremos a las Directrices del G29 anteriormente mencionadas, que tienen como primer objetivo aclarar esta noción y ofrecer criterios para las listas que deben adoptar las autoridades de protección de datos (APD) en virtud del artículo 35, apartado 4.

La EIPD se debe hacer en algunos supuestos que el artículo 35.3 del RGPD describe de manera genérica y que el legislador ha considerado que pueden dar lugar a riesgos elevados, si bien el artículo mencionado utiliza la expresión «en particular», con lo que se deduce que no estamos ante una lista exhaustiva; por lo tanto, hay otros tipos de tratamientos que no encajan en estos supuestos y que también pueden presentar riesgos igualmente elevados y, en consecuencia, habría que hacer la EIPD. Por este motivo, en las Directrices mencionadas del GT 29 se han desarrollado una serie de criterios que van más allá de una simple explicación de lo que debería entenderse a partir de los tres ejemplos indicados en el artículo 35, apartado 3 del RGPD.

En realidad, con el fin de ofrecer un conjunto más concreto de operaciones de tratamiento que requieran una EIPD, teniendo en cuenta los elementos particulares del artículo 35, apartado 1, y del artículo 35, apartado 3, letras a) a c), la lista que debe adoptarse a nivel nacional en virtud del artículo 35, apartado 4, y los considerandos 71,

Boletín de la Asociación Internacional de Derecho Cooperativo
ISSN: 1134-993X • ISSN-e: 2386-4893, No. 56/2020, Bilbao, págs. 47-72
doi: http://dx.doi.org/10.18543/baidc-56-2020pp47-72 • http://www.baidc.deusto.es

75 y 91, y otras referencias del RGPD a operaciones de tratamiento que «probablemente entrañen un alto riesgo», en las Directrices del GT29 (pp. 10-14) se han introducido hasta nueve criterios que pueden evidenciar un elevado riesgo inherente a las operaciones de tratamiento y que, por lo tanto, pueden indicar que hay que llevar a cabo la EIPD. También se han incluido algunos ejemplos de aplicación de estos criterios para determinar si la EIPD es obligatoria.

Los criterios recogidos en el documento del GT29 son los siguientes:

1. Evaluación o puntuación, incluida la elaboración de perfiles y la predicción, especialmente de «aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado» (considerandos 71 y 91). Algunos ejemplos de esto podrán incluir a una institución financiera que investigue a sus clientes en una base de datos de referencia de crédito o en una base de datos contra el blanqueo de capitales y la financiación del terrorismo o sobre fraudes, o a una empresa de biotecnología que ofrezca pruebas genéticas directamente a los consumidores para evaluar y predecir los riesgos de enfermedad/salud, o a una empresa que elabore perfiles de comportamiento o de mercadotecnia basados en el uso o navegación en su sitio web.
2. Toma de decisiones automatizada con efecto jurídico significativo o similar: tratamiento destinado a tomar decisiones sobre los interesados que produce «efectos jurídicos para las personas físicas» o que les afectan «significativamente de modo similar» [artículo 35, apartado 3, letra a)]. Por ejemplo, el tratamiento puede provocar exclusión o discriminación contra las personas.
3. Observación sistemática: tratamiento usado para observar, supervisar y controlar a los interesados, incluidos los datos recogidos a través de redes u «observación sistemática [...] de una zona de acceso público» [artículo 35, apartado 3, letra c)]. Este tipo de observación representa un criterio porque los datos personales pueden ser recogidos en circunstancias en las que los interesados pueden no ser conscientes de quién está recopilando sus datos y cómo se usarán. Además, puede resultar imposible para las personas evitar ser objeto de este tipo de tratamiento en espacios públicos (o espacios de acceso público).
4. Datos sensibles o datos muy personales: esto incluye las categorías especiales de datos personales definidas en el artículo 9

(por ejemplo, información sobre las opiniones políticas de las personas), así como datos personales relativos a condenas e infracciones penales según la definición del artículo 10. Un ejemplo sería un hospital general que guarda historiales médicos de pacientes o un investigador privado que guarda datos de delincuentes. Más allá de estas disposiciones del RGPD, puede considerarse que algunas categorías de datos aumentan el posible riesgo para los derechos y libertades de las personas. Estos datos personales se consideran sensibles (dado que este término es de uso común) porque están vinculados a hogares y actividades privadas (como comunicaciones electrónicas cuya confidencialidad debe ser protegida), porque afectan al ejercicio de un derecho fundamental (como datos de localización cuya recogida compromete la libertad de circulación) o porque su violación implica claramente graves repercusiones en la vida cotidiana del interesado (como datos financieros que podrían usarse para cometer fraude en los pagos). En este sentido, puede resultar relevante que los datos ya se hayan hecho públicos por el interesado o por terceras personas. El hecho de que los datos personales sean de acceso público puede considerarse un factor en la evaluación si estaba previsto que estos se usaran para ciertos fines. Este criterio también puede incluir datos tales como documentos personales, correos electrónicos, diarios, notas de lectores de libros electrónicos equipados con opciones para tomar notas e información muy personal incluida en aplicaciones de registro de actividades vitales (en relación con los datos en las relaciones laborales, puede verse: MERCADER, 2018,42).

5. Tratamiento de datos a gran escala: el RGPD no define qué se entiende por gran escala, aunque el considerando 91 ofrece alguna orientación. En cualquier caso, el GT29 recomienda que se tengan en cuenta los siguientes factores, en particular, a la hora de determinar si el tratamiento se realiza a gran escala: el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente; el volumen de datos o la variedad de elementos de datos distintos que se procesan; la duración o permanencia de la actividad de tratamiento de datos; o el alcance geográfico de la actividad de tratamiento.
6. Asociación o combinación de conjuntos de datos, por ejemplo procedentes de dos o más operaciones de tratamiento de datos realizadas para distintos fines o por responsables del trata-

Boletín de la Asociación Internacional de Derecho Cooperativo
ISSN: 1134-993X • ISSN-e: 2386-4893, No. 56/2020, Bilbao, págs. 47-72
doi: http://dx.doi.org/10.18543/baidc-56-2020pp47-72 • http://www.baidc.deusto.es

miento distintos de una manera que exceda las expectativas razonables del interesado.

7. Datos relativos a interesados vulnerables (considerando 75): El tratamiento de este tipo de datos representa un criterio debido al aumento del desequilibrio de poder entre los interesados y el responsable del tratamiento, lo cual implica que las personas pueden ser incapaces de autorizar o denegar el tratamiento de sus datos, o de ejercer sus derechos. Entre los interesados vulnerables puede incluirse a niños (se considera que no son capaces de denegar o autorizar consciente y responsablemente el tratamiento de sus datos), empleados, segmentos más vulnerables de la población que necesitan una especial protección (personas con enfermedades mentales, solicitantes de asilo, personas mayores, pacientes, etc.), y cualquier caso en el que se pueda identificar un desequilibrio en la relación entre la posición del interesado y el responsable del tratamiento.
8. Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas, como combinar el uso de huella dactilar y reconocimiento facial para mejorar el control físico de acceso, etc. El RGPD deja claro (artículo 35, apartado 1, y considerandos 89 y 91) que el uso de una nueva tecnología, definida «en función del nivel de conocimientos técnicos alcanzado» (considerando 91), puede hacer necesario realizar una EIPD. Esto es debido a que el uso de dicha tecnología puede implicar nuevas formas de recogida y utilización de datos, posiblemente con un alto riesgo para los derechos y libertades de las personas. De hecho, las consecuencias personales y sociales del despliegue de una nueva tecnología pueden ser desconocidas. Por ello, una EIPD ayudará al responsable del tratamiento a entender y abordar tales riesgos. Por ejemplo, algunas aplicaciones del «Internet de las cosas» podrían tener un impacto significativo sobre la vida diaria y la privacidad de las personas y, por tanto, requieren una EIPD.
9. Cuando el propio tratamiento «impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato» (artículo 22 y considerando 91). Esto incluye operaciones de tratamiento destinadas a permitir, modificar o denegar el acceso de los interesados a un servicio o a un contrato. Un ejemplo de esto sería cuando un banco investiga a sus clientes en una base de datos de referencia de crédito con el fin de decidir si les ofrece un préstamo.

El GT 29 entiende que un responsable del tratamiento puede considerar que un tratamiento que cumpla dos criterios requerirá la realización de una EIPD.

Ejemplos de tratamiento que requieren EIPD:

1. Un hospital que trata los datos genéticos y sanitarios de sus pacientes. Criterios que la justifican: datos sensibles o datos muy personales; datos relativos a interesados vulnerables y tratamiento de datos a gran escala.
2. Una empresa que observa sistemáticamente las actividades de sus empleados, incluida la observación del puesto de trabajo de los empleados, la actividad en internet, etc. Criterios que la justifican: observación sistemática y datos relativos a interesados vulnerables.
3. Una institución que crea una base de datos nacional de calificación crediticia o sobre fraudes. Criterios que la justifican: evaluación o puntuación; toma de decisiones automatizada con efecto jurídico significativo o similar; imposibilidad para los interesados de ejercer un derecho o utilizar un servicio o ejecutar un contrato y datos sensibles o datos muy personales.

Ejemplos de tratamiento que no requieren EIPD:

1. Un tratamiento de «datos personales de pacientes o clientes por un solo médico, otro profesional de la salud o abogado» (considerando 91) No se considera suficiente la existencia de datos sensibles o datos muy personales o de datos relativos a interesados vulnerables.
2. Una revista en línea que use una lista de distribución para enviar un resumen diario genérico a sus suscriptores. No se considera suficiente la existencia de un tratamiento de datos a gran escala.

2. *Constitución de equipo de trabajo y definición de sus términos de referencia*

Con carácter previo al inicio de las tareas para llevar a cabo una EIPD es conveniente reflexionar sobre quiénes deben ser los encargados de realizarla y los resultados esperados de su trabajo.

El GT 29 señala que la obligación de hacer una EIPD corresponde al responsable del tratamiento, con el apoyo y la colaboración del encargado del tratamiento y del delegado de protección de datos. Asi-

Boletín de la Asociación Internacional de Derecho Cooperativo
ISSN: 1134-993X • ISSN-e: 2386-4893, No. 56/2020, Bilbao, págs. 47-72
doi: http://dx.doi.org/10.18543/baidc-56-2020pp47-72 • http://www.baidc.deusto.es

mismo, impone al delegado de protección de datos el deber de controlar la realización de la EIPD [artículo 39, apartado 1, letra c)].

Con relación a las reglas de composición del equipo o grupo de trabajo, no existe ninguna con el carácter de predeterminadas, por lo que cada organización es libre de establecerlas en función de sus propias estructuras y competencias de funcionamiento. Es importante, no obstante, tal como señala la AEPD, que se trate de un equipo o grupo de carácter multidisciplinar, donde pueden recogerse los criterios de personas con diferente formación y visión, en el análisis de los datos y del tratamiento que se pretende llevar a efecto.

La propia AEPD también señala que la obligación de hacer una EIPD corresponde al responsable del tratamiento, con el apoyo y la colaboración del encargado del tratamiento, si lo hubiese, y en su caso, con el Delegado de Protección de Datos.

Adicionalmente, el personal encargado de la seguridad, el área de tecnología, asesoría jurídica o incluso diferentes responsables de distintas áreas implicadas en el tratamiento pueden ser requeridos durante el proceso de evaluación.

En lo que respecta a la ejecución de la EIPD, la AEPD señala que puede realizarse por personal interno o externo de la organización, sin que esto exima del cumplimiento de sus obligaciones al responsable del tratamiento, que debe asegurar que esta se haga de forma adecuada y se implanten los controles y medidas de control resultantes de la evaluación.

La participación del Delegado de Protección de Datos (DPD) en la elaboración debe entenderse como una función de asesoramiento, considerando que el DPD, entre sus funciones, debe responder a las consultas que surjan y monitorizar el proceso.

Finalmente, el RGPD prevé que cuando resulte procedente se deberá recabar la opinión de los interesados o de sus representantes, sin perjuicio de que se adopten las medidas necesarias para proteger intereses comerciales o de negocio. La consulta con terceras partes encargadas de las actividades de tratamiento proporciona a la Organización la oportunidad de obtener una visión completa de cómo se verán afectados los datos por las actividades de tratamiento delegadas en terceros. Entre las posibles garantías para los derechos y libertades de los interesados deberá estimarse la posibilidad que el RGPD recoge también en su artículo 35.9 de pedir, cuando proceda, las opiniones de los interesados o sus representantes. En el ámbito interno sería razonable entender que las consultas deben centrarse en los departamentos de TIC, los grupos de personal especializado para el manejo de la información personal, como: (i) personal de la empresa; (ii) personal de gestión de

la información o de recursos; (iii) áreas de compras; (iv) de contratación; (v) de gestión de cobros; (vi) de investigación del fraude; (vii) de atención al público; (viii) de comunicación; (ix) de cumplimiento y gobernanza; (x) de las áreas de seguridad de la propia organización; (xi) de las áreas de marketing y de comunicación de la empresas; (xii) de las áreas de negocio afectadas, que puedan entender de manera adecuada los objetivos de negocios propuestos, y que tengan pleno conocimiento de las medidas que se han de adoptar, y cuando han de llevarse a efecto; (xiii) y obviamente, de la alta dirección, y, aunque no son estrictamente agentes internos, los encargados de tratamiento, si los hubiere, y aquellos proveedores cuya participación pudiera resultar relevante.

Un ejemplo del grupo de trabajo sería el formado por el responsable del Departamento de Recursos Humanos, del Departamento de Sistemas de la Información y Responsable de Seguridad, del Departamento de Administración, del de calidad, así como el Delegado de Protección de Datos y un asesor externo especialista en protección de datos (PUYOL, 2018, 41).

Respecto a la opinión de los interesados, en el proceso de Evaluación de Impacto es recomendable llevar a cabo consultas con partes que se vayan a ver afectadas por dicho tratamiento, bien sean estas de carácter externo o interno a la propia organización, con el objetivo de poder identificar oportuna y de manera correcta los riesgos que se puedan producir.

En ese sentido, consideramos relevante consultar con las personas previamente señaladas, mediante una entrevista que debe quedar documentada en un cuestionario tipo que permita analizar los riesgos en materia de protección de datos de carácter personal.

3. *Descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento*

Como punto de partida, es necesario conocer en detalle todo el ciclo de vida y el flujo de los datos personales y todos los actores y elementos que intervienen durante las actividades de tratamiento desde su inicio hasta su fin.

El apartado a) del artículo 35.7 del RGPD establece la obligación de que la EIPD incluya, al menos, una descripción sistemática y detallada del tratamiento. Como resultado de esta etapa, se debe obtener una visión en detalle que permita facilitar la identificación de las amenazas y los riesgos a los que están expuestos los datos de carácter personal asociados al mismo.

Boletín de la Asociación Internacional de Derecho Cooperativo
ISSN: 1134-993X • ISSN-e: 2386-4893, No. 56/2020, Bilbao, págs. 47-72
doi: http://dx.doi.org/10.18543/baidc-56-2020pp47-72 • http://www.baidc.deusto.es

Adicionalmente a la descripción del tratamiento, se debe obtener una descripción clara de los elementos que intervienen en cada una de las fases del ciclo de vida de los datos del tratamiento.

El ciclo de vida de los datos se puede dividir en las siguientes etapas:

1. **Captura de datos:** Dentro de la captura de datos se pueden encontrar diversas técnicas, como por ejemplo: formularios web, formularios en papel, la toma de muestras y realización de encuestas, etc.
2. **Clasificación/ Almacenamiento**: Que consiste en establecer categorías y asignarlas a los datos para su clasificación y almacenamiento en los sistemas o archivos.
3. **Uso/Tratamiento:** Es la operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos automatizados o manuales.
4. **Cesión de los datos a un tercero para su tratamiento**: Que se concreta en el traspaso o comunicación de datos realizada a un tercero (toda persona física o jurídica, pública o privada u órgano administrativo).
5. **Destrucción:** Es eliminar los datos que puedan estar contenidos en los sistemas o archivos, de manera que no puedan ser recuperados de los soportes.

Adicionalmente, para cada una de las etapas del ciclo de vida de los datos en las actividades de tratamiento, se deben identificar todos los elementos involucrados en cada una de las etapas. Podríamos clasificar los elementos involucrados en las siguientes categorías:

1. **Actividades de tratamiento.** Es importante describir en detalle todas las actividades u operaciones que se llevan a cabo sobre los datos de carácter personal con el objetivo de entender los posibles riesgos a los que se pueden ver expuestos los datos.
   Puede considerarse una actividad u operación cualquier tarea que requiera el tratamiento o manipulación de los datos, por ejemplo, la captura de datos mediante un formulario web, el filtrado de información mediante un proceso de perfilado, un proceso de cifrado o el borrado de datos.
2. **Datos tratados.** Se deben identificar los datos de carácter personal tratados o manipulados durante el tratamiento vigilando siempre que los mismos correspondan a los principios que el artículo 5 del RGPD dicta.
   Es necesario considerar el principio de minimización de los datos y asegurar que no existen datos que no se prevén utilizar o

recopilar sin utilidad para la finalidad de las actividades de tratamiento.

3. **Intervinientes involucrados.** Se deben identificar a las personas físicas o jurídicas que, de manera individual o colectiva, están implicadas en el desarrollo de las actividades del tratamiento de los datos de carácter personal. Los intervinientes en el tratamiento deben estar identificados y tener delimitadas sus funciones y responsabilidades.

   Dentro del grupo de los intervinientes se puede incluir el responsable del tratamiento, áreas o empleados de las organizaciones que participan activamente del procesado de los datos, encargados de tratamiento, etc.

4. **Tecnologías intervinientes.** Dentro de cada etapa se debe identificar el hardware y el software que sea relevante desde la perspectiva del tratamiento de los datos de carácter personal. Se debe identificar la tecnología (cloud, BBDD, servidores), aplicaciones, dispositivos y técnicas empleadas en el procesamiento de los datos.

4. *Analisis de la necesidad y proporcionalidad de las operaciones de tratamiento con respecto a su finalidad*

Analizar la necesidad y proporcionalidad de las actividades de tratamiento, requiere plantearse las siguientes cuestiones:

1. **La licitud del tratamiento.** El tratamiento de los datos personales debe ser lícito y, por tanto, es necesario que los datos se traten de acuerdo con las condiciones recogidas en el RGPD. Es fundamental tener clara la base legitimadora en que se basa el tratamiento. En este sentido, el artículo 6 del RGPD, recoge los supuestos en los que se considera que el tratamiento de datos personales es lícito, que son los siguientes:

   — Que se cuente con el consentimiento del interesado para los fines específicos del tratamiento.
   — Que el tratamiento sea necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.
   — Que el tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.
   — Que el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física.

Boletín de la Asociación Internacional de Derecho Cooperativo
ISSN: 1134-993X • ISSN-e: 2386-4893, No. 56/2020, Bilbao, págs. 47-72
doi: http://dx.doi.org/10.18543/baidc-56-2020pp47-72 • http://www.baidc.deusto.es

— Que el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
— Que el tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

2. **Necesidad y proporcionalidad del tratamiento.** El principio de «minimización de datos» establece que los datos personales serán «adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que serán tratados». Durante la definición del mismo, se debe considerar qué datos son estrictamente necesarios para realizar las actividades de tratamiento en función de las finalidades previstas.
Del mismo modo, todas las acciones que el tratamiento incluya deben ser necesarias y proporcionales a las finalidades previstas. Para determinar la necesidad de llevar a cabo un tratamiento, se debe seguir un planteamiento pragmático. Si se toma como base el artículo 39 del RGPD, se deben tener en cuenta los siguientes aspectos para evaluar la necesidad del tratamiento:

1. «Los datos personales sólo se deben tratar si la finalidad del tratamiento no se puede hacer razonablemente por otros medios», es decir, sin tratar datos personales.
2. «Las finalidades tienen que estar definidas de manera determinada, explícita y legítima».
3. «Cualquier tratamiento de datos personales tiene que ser lícito y leal». Este punto está unido al análisis de las finalidades establecidas en el tratamiento y su supuesto legitimador.
4. «Los datos personales tienen que ser adecuados, pertinentes y limitados a lo necesario para los fines para los cuales se tratan».
5. «El plazo de conservación se limite a un mínimo estricto».

La proporcionalidad tiene que ver con evaluar si la finalidad que se persigue se puede conseguir por otros medios, por ejemplo: utilizando otros datos, reduciendo el universo de personas afectadas (de manera cuantitativa o cualitativa), haciendo uso de

otras tecnologías menos invasivas o bien aplicando otros procedimientos o medios de tratamiento (modificando los inicialmente previstos), etc.

A nivel práctico, analizar la proporcionalidad exige responder de manera argumentada a dos preguntas:

— ¿El tratamiento, tal y como está definido, es necesario para la finalidad prevista?
— ¿Las actividades de tratamiento son proporcionales a las finalidades previstas?

5. *Identificación y evaluación de riesgos para la protección de datos*

En esta etapa inicial del proceso de gestión de riesgos se deben identificar los potenciales escenarios de riesgo derivados de un inadecuado tratamiento de sus datos.

El riesgo es la exposición a amenazas, por tanto, como punto de partida, es fundamental entender qué es una amenaza y cómo se puede identificar escenarios de riesgo a partir de la misma.

Una amenaza es cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesados sobre cuyos datos de carácter personal se realiza un tratamiento.

Si ponemos foco en la protección de los datos, las amenazas se pueden categorizar principalmente en tres tipos en base a la tipología de daño que pueden producir en los datos:

— **Acceso ilegítimo a los datos**: confidencialidad.
— **Modificación no autorizada de los datos**: integridad.
— **Eliminación de los datos**: disponibilidad.

Para identificar de forma adecuada las amenazas asociadas a las actividades de tratamiento, se debe tener en cuenta todo el ciclo de vida de los datos en cada operación, desde su inicio hasta el momento en el que finaliza. Identificar una amenaza consiste en identificar la fuente de los escenarios en los que se puede producir un daño o una violación de los derechos y libertades de los interesados.

Cada entidad puede disponer de catálogos estandarizados de amenazas que faciliten el proceso.

Un riesgo se puede definir como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas. El nivel del riesgo se mide según su probabilidad de materializarse y el impacto que tiene en caso de hacerlo.

Boletín de la Asociación Internacional de Derecho Cooperativo
ISSN: 1134-993X • ISSN-e: 2386-4893, No. 56/2020, Bilbao, págs. 47-72
doi: http://dx.doi.org/10.18543/baidc-56-2020pp47-72 • http://www.baidc.deusto.es

Para evaluar un riesgo es necesario considerar todos los posibles escenarios con los que el riesgo se haría efectivo, incluidos aquellos que impliquen un mal uso o abuso de los datos y las alteraciones técnicas o del entorno.

Las amenazas y los riesgos asociados están directamente relacionados, en consecuencia, identificar y evaluar los riesgos siempre implica considerar la amenaza que los puede originar.

Ejemplos prácticos de amenazas y su relación con el riesgo y su posible impacto:

Ejemplo n.º1 (acceso ilegítimo a los datos): La pérdida de un dispositivo móvil o la fuga de información (amenaza), podría derivar en un acceso por parte de personal no autorizado a los datos y, en consecuencia, se produciría una vulneración de los derechos y libertades de los interesados (riesgo), lo que podría derivar en un posible daño moral, físico o material sobre el interesado (impacto).

Ejemplo n.º 2 (modificación no autorizada de los datos): La ausencia de mecanismos de control en un sistema es una vulnerabilidad que puede facilitar una suplantación de identidad derivada de un ataque cibernético (amenaza). El ataque puede provocar una modificación no autorizada de datos que altere la integridad y disponibilidad de los datos (riesgo), con la posibilidad de provocar daños y perjuicios, materiales a los interesados (impacto).

6. *Evaluación y gestión de riesgos: riesgos inherentes, medidas mitigadoras y riesgos residuales*

La evaluación de riesgos consiste en valorar y estimar la probabilidad y el impacto de que el riesgo se materialice.

El riesgo inherente es el riesgo intrínseco de cada actividad, sin tener en cuenta las medidas de control que mitigan o reducen su nivel de exposición. El riesgo inherente surge de la exposición que se tenga a la operación de tratamiento en particular y de la probabilidad de que la amenaza asociada al riesgo se materialice. El cálculo del riesgo inherente se realiza mediante la siguiente fórmula:

Riesgo = Probabilidad x Impacto

La escala de posibles valores para el cálculo de la probabilidad es la siguiente:

Probabilidad despreciable: La posibilidad de ocurrencia es muy baja (por ejemplo, un evento que puede pasar de forma fortuita).
Probabilidad limitada: La posibilidad de ocurrencia es baja (por ejemplo, un evento que puede pasar de forma ocasional).
Probabilidad significativa: La posibilidad de ocurrencia es alta (por ejemplo, un evento que puede pasar con bastante frecuencia).
Probabilidad máxima: La posibilidad de ocurrencia es muy elevada (por ejemplo, un evento cuya ocurrencia se produce con mucha frecuencia).

El impacto se determina en base a los posibles daños que se pueden producir si la amenaza se materializa. De igual modo, el impacto también se evaluará con la misma escala de cuatro valores posibles:

Impacto despreciable: El impacto es muy bajo (por ejemplo, un evento cuyas consecuencias son prácticamente despreciables sin impacto sobre el interesado).
Impacto limitado: El impacto es bajo (por ejemplo, un evento cuyas consecuencias implican un daño menor sin impacto relevante sobre el interesado).
Impacto significativo: El impacto es alto (por ejemplo, un evento cuyas consecuencias implican un daño elevado con impacto sobre el interesado).
Impacto máximo: El impacto es bajo (por ejemplo, un evento cuyas consecuencias implican un daño muy elevado con un impacto crítico sobre el interesado).

El impacto asociado a un riesgo puede ser ocasionado por daños de diferente índole, saber:

Daño físico: Conjunto de acciones que pueden ocasionar un daño en la integridad física del interesado.
Daño material: Conjunto de acciones que pueden ocasionar pérdidas económicas, de patrimonio, de empleo, etc.
Daño moral: Conjunto de acciones que pueden ocasionar un daño moral o mental en el interesado, como una depresión, fobias, acoso, etc.

Para poder determinar el **riesgo inherente**, es necesario asignar valores a cada uno de los niveles de las escalas de probabilidad e impacto. La escala de valores comprende desde el valor 1, en el caso de

Boletín de la Asociación Internacional de Derecho Cooperativo
ISSN: 1134-993X • ISSN-e: 2386-4893, No. 56/2020, Bilbao, págs. 47-72
doi: http://dx.doi.org/10.18543/baidc-56-2020pp47-72 • http://www.baidc.deusto.es

que la magnitud sea despreciable, hasta el valor 4 en el caso donde la magnitud es máxima:

— **IMPACTO:**

- Despreciable 1
- Limitado 2
- Significativo 3
- Máximo 4

— **PROBABILIDAD:**

- Máxima 1
- Significativa 2
- Limitada 3
- Despreciable 4

Si se establece un valor numérico a la probabilidad y otro valor al impacto, según la escala de valores definida, se obtiene una posición en la matriz de riesgos que se corresponde con el riesgo inherente resultado de aplicar la fórmula de estimación del riesgo. El resultado del riesgo inherente se puede considerar en los siguientes niveles en función del valor obtenido:

Bajo: Si el valor resultante se sitúa entre los valores 1 y 2.
Medio: Si el valor resultante es mayor de 2 y menor o igual que 6.
Alto: Si el valor resultante es mayor que 6 y menor o igual que 9.
Muy Alto: Si el valor resultante es mayor que 9.

Considerando los criterios establecidos, si se deseara valorar un riesgo, por ejemplo, al añadir valores numéricos a la probabilidad y al impacto, ante un riesgo con probabilidad limitada (2) e impacto significativo (3), el nivel de riesgo inherente será medio (2 x 3 = 6).

Durante la fase de evaluación de riesgos, se debe realizar este ejercicio para cada una de las amenazas identificadas, considerando los riesgos asociados, el impacto y la probabilidad de que se materialice y determinando su riesgo inherente.

La última etapa del proceso de gestión de riesgos consiste en definir la respuesta o las medidas necesarias para tratar el riesgo y reducir su nivel de exposición. Tratar un riesgo es el resultado de definir y establecer medidas de control para disminuir la probabilidad y/o el impacto asociados al riesgo inherente de una operación de tratamiento.

Las medidas de control tienen como objetivo mitigar o minimizar el riesgo asociado a una operación de tratamiento. Es importante

destacar que el objetivo principal de una EIPD no es eliminar completamente el riesgo asociado a las actividades de tratamiento, lo que se pretende es reducir el mismo hasta un nivel aceptable para poder llevar a cabo las mismas garantizando los derechos y libertades de los interesados.

El riesgo residual es el riesgo de cada actividad una vez se hayan aplicado las medidas de control para mitigar y/o reducir su nivel de exposición. A diferencia del riesgo inherente, el riesgo residual contempla las medidas de control definidas sobre la actividad de tratamiento para valorar la probabilidad y/o el impacto asociado al riesgo.

Para evaluar el riesgo residual, se debe estimar de nuevo la probabilidad y el impacto considerando las medidas de control definidas, mediante la siguiente fórmula:

Riesgo residual = Probabilidad x Impacto

Por tanto, sobre esos parámetros deberá realizarse la evaluación de riesgos por cada empresa.

7. *Conclusión*

Como último paso en la realización de una EIPD, se debe elaborar un plan de acción donde se describan todas las medidas de control definidas para tratar los riesgos identificados y concluir con respecto al resultado obtenido.

8. *Supervisión y revisión de la implantación*

La EIPD permite determinar las medidas de control necesarias para tratar los riesgos identificados. Sin embargo, no deja de ser un ejercicio teórico que requiere su puesta en práctica de forma íntegra para garantizar los derechos y las libertades de los interesados.

A nivel práctico, es recomendable que una figura delegada supervise y garantice que las medidas de control definidas durante la EIPD se implantan adecuadamente antes de llevar a cabo las actividades de tratamiento de datos de carácter personal por parte del responsable del tratamiento.

Boletín de la Asociación Internacional de Derecho Cooperativo
ISSN: 1134-993X • ISSN-e: 2386-4893, No. 56/2020, Bilbao, págs. 47-72
doi: http://dx.doi.org/10.18543/baidc-56-2020pp47-72 • http://www.baidc.deusto.es

IV. **Sanción por incumplir con la obligación de realizar la evaluación de impacto relativa a la protección de datos**

La realización del análisis descrito y realizarlo correctamente, con el asesoramiento adecuado, es importante para todas las empresas, incluidas las sociedades cooperativas. La no realización de la Evaluación de Impacto relativa a la Protección de Datos cuando sea obligatoria para el responsable del tratamiento en atención a los datos personales tratados o no hacerlo de manera correcta, podría suponer la comisión de una infracción que podría ser sancionada, cuando se trate de empresas, con multa administrativa hasta de diez millones de euros (10.000.000 €) o hasta una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía (artículo 83.4 del RGPD).

Bibliografía

AGENCÍA ESPAÑOLA DE PROTECCIÓN DE DATOS, «Guía del Reglamento General de Protección de Datos para responsables de tratamiento», https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

AGENCÍA ESPAÑOLA DE PROTECCIÓN DE DATOS, «Guía para el cumplimiento del deber de informar», https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf

AGENCÍA ESPAÑOLA DE PROTECCIÓN DE DATOS, «Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD», https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

AUTORIDAD CATALANA DE PROTECCIÓN DE DATOS, «Guía Práctica: Evaluación de impacto protección de datos personales», https://apdcat.gencat.cat/.../GUIA-EVALUACION-DE-IMPACTO-CAST-2.0.pdf

GRUPO PROTECCIÓN DE DATOS DEL ARTÍCULO 29, WP 248, «Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679», https://www.aepd.es/media/criterios/wp248rev01-es.pdf

LÓPEZ CALVO, José. 2017. *Comentarios al Reglamento Europeo de protección de Datos*. Las Rozas (Madrid): Editorial Sepín.

MERCADER UGUINA, Jesús R. 2019. *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, 3.ª ed., Francis Lefebre, Madrid, 2019.

MUÑOZ DEIROS, Eva. 2014. «La Privacidad desde el Diseño y las Evaluaciones de Impacto en la Protección de Datos». 31 de octubre de 2014, http://evamunoz.es/privacidad-desde-diseno-evaluaciones-impacto-protecciondatos/.

NIETO MARTÍN, Adán. 2015. «El cumplimiento normativo». En *Manual de cumplimiento penal en la empresa*, 25-48. Valencia: Editorial Tirant Lo Blanch. https://dialnet.unirioja.es/servlet/articulo?codigo=4959230.

PUYOL, Javier. 2018. *El modelo de evaluación de riesgos en la protección de datos EIPD / PIA's*. Valencia: Tirant lo Blanch, 2018.

RECIO GAYO, Miguel. 2016. «Aproximación basada en el riesgo, Evaluación de Impacto relativa a la protección de datos personales y consulta previa a la autoridad de control». En *Reglamento General de protección de Datos. Hacia un nuevo modelo europeo de privacidad*, 351-366. Madrid: Editorial Reus.

Boletín de la Asociación Internacional de Derecho Cooperativo
ISSN: 1134-993X • ISSN-e: 2386-4893, No. 56/2020, Bilbao, págs. 47-72
doi: http://dx.doi.org/10.18543/baidc-56-2020pp47-72 • http://www.baidc.deusto.es

Boletín de la Asociación Internacional de Derecho Cooperativo
ISSN: 1134-993X • ISSN-e: 2386-4893, No. 56/2020, Bilbao, págs. 1-162
http://www.baidc.deusto.es

Derechos de autor

Copyright