Autoritat Catalana de Protecció de Dades

GUÍA PRÁCTICA

(enero de 2018 – versión 2.0)

Evaluación de impacto relativa a la protección de datos

Orientaciones prácticas para hacer las evaluaciones de impacto que prevé 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 y la libre circulación de datos personales

ÍNDICE DE CONTENIDOS

INTRODUCCIÓN: el contexto de esta guía

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 y la libre circulación de datos personales, en definitiva el Reglamento general de protección de datos (en adelante RGPD), incorpora una nueva obligación para los responsables de tratamientos: evaluar el impacto de las operaciones de tratamiento en la protección de los datos personales, cuando sea probable que el tratamiento comporte un riesgo significativo para los derechos y las libertades de las personas.

El RGPD entró en vigor el 24 mayo de 2016 y será de plena aplicación a partir del 25 de mayo de 2018. Durante este periodo de dos años, los responsables y encargados de tratamientos deben 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 general, la reforma de la protección de datos en Europa propone un modelo de cumplimiento orientado a la gestión, que supere el modelo previo, de cariz demasiado formalista en algunos de sus aspectos. De la nueva regulación se destaca el hecho de que será necesario demostrar que se cumplen las obligaciones, y precisamente las evaluaciones de impacto relativas a la protección de los datos de carácter personal (en adelante EIPD) se sitúan en el punto de partida para demostrar una gestión responsable de los tratamientos.

La ejecución de las EIPD se tendrá que sustentar en metodologías o métodos sistemáticos, para que resulten objetivas, repetibles, comparables y estén documentadas. Por eso, los contenidos de esta guía tienen como finalidad orientar en la manera de abordar la ejecución de las evaluaciones de impacto según lo que prevén el RGPD.

Esta es la segunda versión de la guía. La primera se presentó en junio de 2017, y ya incorporaba las directrices del Grupo del artículo 29 en relación con las evaluaciones de impacto.

La revisión de las mencionadas directrices en octubre de 2017 (WP 248, rev.01), junto con otros trabajos del mismo Grupo y de diversas autoridades europeas en esta materia, así como la publicación en junio de 2017 de la ISO / IEC 29134 "Directrices para la evaluación de impacto sobre la privacidad", motivan esta segunda versión.

En esta nueva versión de la guía, la APDCAT también ha incorporado una serie de actualizaciones y mejoras que tienen en cuenta los comentarios que, desde que se publicó en su primera versión, han hecho los responsables de tratamientos y profesionales de la protección de datos que la han aplicado o analizado; esta guía sigue siendo una de las primeras guías de evaluación de impacto publicadas por una autoridad de protección de datos en Europa, tras la aprobación del RGPD.

Por supuesto, los contenidos de esta guía se continuarán revisando y actualizando, de acuerdo con el desarrollo normativo que genere el RGPD, su plena aplicación y las diferentes directrices y trabajos del GT29 o del Comité Europeo de Protección de Datos, así como su aplicación práctica.

A fin de facilitar el seguimiento de los cambios que incorpora esa versión, las modificaciones más relevantes se señalan convenientemente, con una nota a pie de página, con la expresión: "Incorporado en la versión 2.0 de esta guía.", o equivalente.

PARTE 1

Las evaluaciones de impacto relativas a la protección de datos

ASPECTOS GENERALES DE LAS EVALUACIONES DE IMPACTO

Las evaluaciones de impacto se sitúan en el ámbito de las medidas o acciones preventivas, puesto que se trata de un proceso de evaluación que se debe hacer antes de iniciar las operaciones de tratamiento de los datos personales; en este sentido, conecta con el concepto de privacidad en el diseño (*privacy by design*), que en el RGPD se identifica como "protección de datos desde el diseño". Esto supone que, tanto en el momento de definir las diferentes operaciones de tratamiento como en el de determinar y aplicar los medios que se utilizarán para tratar los datos personales, se tendrán en cuenta los principios, los derechos y las obligaciones que recoge la normativa que sea de aplicación a los tratamientos que se pretenden llevar a cabo. Todo esto, desde la necesidad de gestionar los riesgos que pueden suponer las operaciones de tratamiento para los derechos y las libertades fundamentales.

A pesar de lo mencionado en el párrafo anterior, no hay obstáculo para plantear una EIPD para tratamientos ya existentes. De hecho, la evaluación de impacto se debe hacer siguiendo un método que permita repetirla, puesto que en determinadas circunstancias habrá que revisarla y actualizarla.

En cualquier caso, a todos los efectos, la potencialidad y utilidad más grande de los procesos de evaluación se producirá cuando se apliquen durante el diseño de la solución, siempre en paralelo a la definición de los procesos de tratamiento y, por supuesto, antes de hacer su implementación.

También resulta conveniente tener en cuenta que las EIPD son un instrumento muy útil en relación con el principio de responsabilidad proactiva *(accountability)*, puesto que facilita no sólo cumplir la norma, sino también poderlo demostrar.

Así lo explicita el GT29 en el WP 248[1] «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) 2016/279», cuando se refiere a las evaluaciones de impacto como herramientas importantes para la rendición de cuentas, puesto que no sólo ayudan los responsables a cumplir los requisitos del RGPD, sino que también permiten demostrar que han adoptado las medidas adecuadas para garantizar el cumplimiento del Reglamento: [2]*"una EIPD es un proceso utilizado para reforzar y demostrar el cumplimiento".*

[1] Disponible en http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.
[2] Incorporado en la versión 2.0 de esta guía

.

Precisamente en base al principio de responsabilidad activa, el RGPD es flexible en cuanto a la manera de llevar a cabo la evaluación de impacto; en consecuencia, podremos adoptar un método desarrollado por terceros (una autoridad de control, un organismo de estandarización, un sector empresarial, una asociación, etc.) o bien aplicar un método propio, siempre que el resultado de la evaluación cumpla con los requisitos, los contenidos mínimos y las finalidades que prevé el RGPD.

[3]Independientemente de la metodología de evaluación empleada, esta debe implicar una verdadera estimación de los riesgos, que permita a los responsables del tratamiento decidir las medidas más adecuadas para afrontarlos; depende de los responsable del tratamiento elegir una metodología que cumpla con los requisitos y objetivos previstos en el RGPD.

Tal como ha expresado el GT29, la evaluación de impacto es un proceso orientado a describir en detalle las operaciones de tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades que pueden resultar, evaluándolos e identificando las medidas más adecuadas para abordarlos.

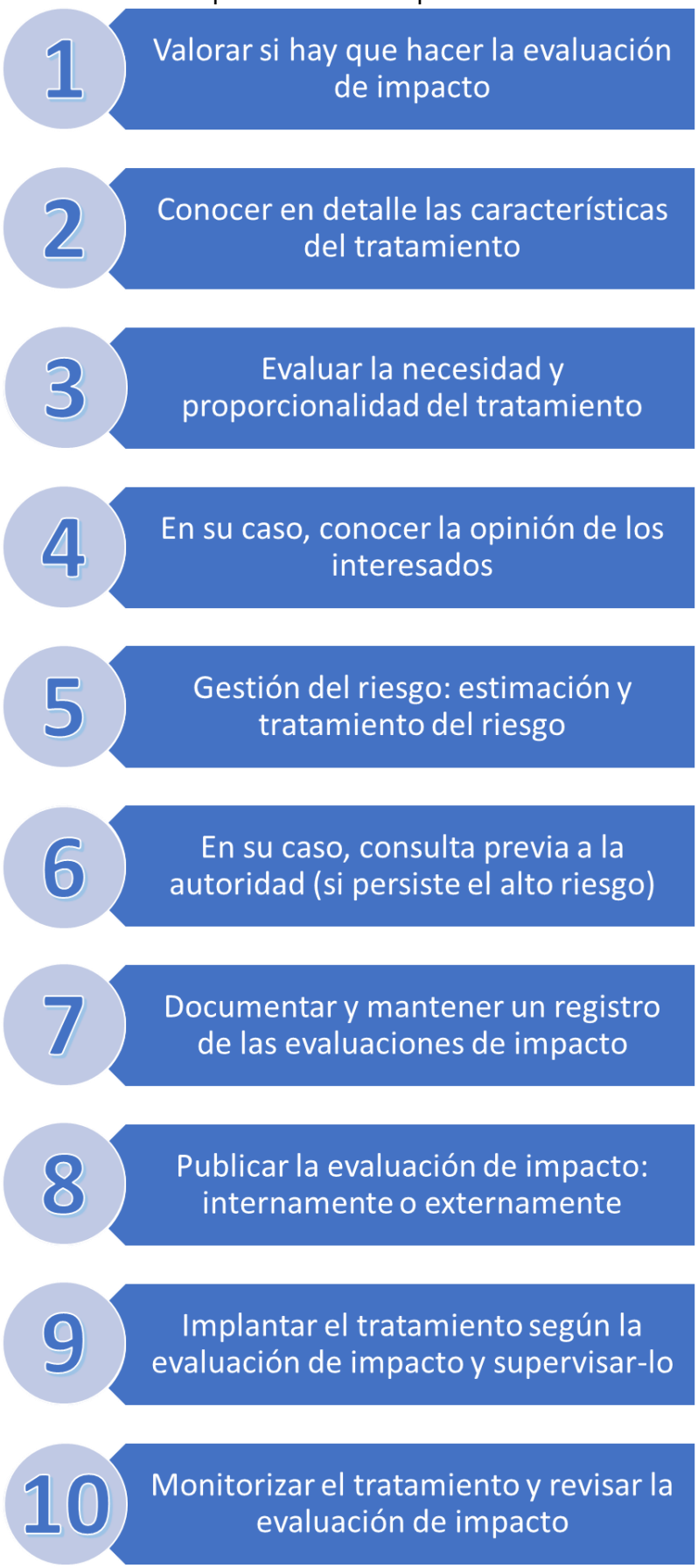
El resultado de la evaluación de impacto se debe tener en cuenta, necesariamente, en el momento de tomar las decisiones relacionadas con el cumplimiento de lo que prevé el RGPD.

Una cuestión importante es que el responsable del tratamiento tiene que consultar a la autoridad de protección de datos competente, si como consecuencia del resultado de la evaluación se llega a la conclusión de que las operaciones de tratamiento implican un alto riesgo que no se puede mitigar (gestionar o controlar) de acuerdo con la tecnología disponible, o bien por los costes o dificultades de implantación de las medidas necesarias para reducir los riesgos. Por supuesto, esta consulta se debe hacer antes de iniciar las operaciones de tratamiento que generan estos riesgos.

En definitiva, las EIPD están orientadas a asegurar preventivamente que, cuando las operaciones de tratamiento puedan comportar riesgos especialmente relevantes (alto riesgo), se tomen medidas para reducir, dentro de lo posible, el riesgo de dañar o perjudicar a las personas, o afectar negativamente sus derechos y libertades, impidiendo o limitando su ejercicio o contenido.

[3] Incorporado en la versión 2.0 de esta guía

Conceptualmente podemos resumir la evaluación de impacto relativa a los datos personales en 10 pasos



LAS EVALUACIONES DE IMPACTO EN EL RGPD

El considerando 84 del Reglamento 2016/679 recoge que, para mejorar el cumplimiento del RGPD, el responsable del tratamiento debe realizar una evaluación de impacto (EIPD) relativa a la protección de datos cuando un tratamiento, por su naturaleza, alcance, contextos o finalidades, y particularmente si utiliza nuevas tecnologías, potencialmente pueda comportar un alto riesgo para los derechos y las libertades de las personas físicas. La evaluación se debe hacer antes de iniciar el tratamiento y tiene que valorar el origen, la naturaleza, la particularidad y la gravedad del riesgo.

Entonces, como criterio general se debe tener presente que la introducción de tecnologías emergentes, o de nuevos usos de las tecnologías, es particularmente relevante al tomar la decisión de llevar a cabo la EIPD. En consecuencia, se debe prestar especial atención a las características de estas nuevas tecnologías, o a la manera en que se pretenden utilizar.

El RGPD deja abierta la posibilidad de abordar un conjunto de operaciones de procesamiento similares, que presenten riesgos similares, con una sola evaluación; como consecuencia, no hay inconveniente en que la evaluación alcance diferentes tratamientos, por ejemplo debido a su coste de realización. El considerando 92 hace referencia y expone que hay circunstancias en que puede ser razonable y económico que una evaluación de impacto relativa a la protección de datos incluya más de un proyecto, y hace mención a varios ejemplos en que puede ser adecuado efectuar una EIPD conjunta.

[4]En esos supuestos el GT29 recomienda hacer pública una EIPD de referencia, y que se expliquen motivadamente las razones que han llevado a hacer una única evaluación de impacto que aplica a diferentes tratamientos.

Otra cuestión que también recoge el WP 248 del GT29 es que, cuando la EIPD afecta a operaciones de tratamiento efectuadas conjuntamente por varios responsables de tratamiento, la evaluación tiene que determinar con precisión a quien corresponde implantar las diferentes medidas resultantes de la evaluación de impacto.

También se puede dar el caso que la EIPD se lleve a cabo respecto de una solución de software, o incluso en relación con un dispositivo, o producto tecnológico, que muy

[4] Incorporado en la versión 2.0 de esta guía

probablemente diferentes responsables de tratamientos utilizarán en sus respectivas actividades de tratamiento, y en diferentes tipologías de tratamientos.

En ese caso, la evaluación de impacto de la solución o del producto también puede ser útil para evaluar el impacto del tratamiento, aunque obviamente habrá que hacer la EIPD respecto de la implementación específica de la solución de software o de hardware, [5]ya que el responsable del tratamiento sigue teniendo la obligación de hacer su propia EIPD, que por supuesto se puede hacer a partir de la evaluación hecha por el proveedor del producto o solución tecnológica.

Hay que tener presente que la evaluación no es obligatoria para todos los tratamientos, sino sólo para los que comportan un riesgo elevado o especialmente relevante, que se traduce en la expresión "alto riesgo".

En este sentido, como veremos, lo primero que hay que analizar es si se debe ejecutar la evaluación de impacto para un nuevo tratamiento que se esté planteando llevar a cabo[6].

La regulación material de las EIPD se sitúa principalmente en el artículo 35 del RGPD, mientras que las consultas previas se regulan en el artículo 36.

¿Cuándo se debe hacer la evaluación de impacto?

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. 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.

La determinación de si se tiene que llevar a cabo una EIPD está muy vinculada a dos conceptos que no están formalmente definidos en el Reglamento: “el alto riesgo”, al cual ya hemos hecho referencia, y el de "tratamiento a gran escala".

[5] Incorporado en la versión 2.0 de esa guía
[6] El proyecto de Ley Orgánica de Protección de Datos prevé esta obligación en su artículo 28.1

En relación con el alto riesgo, el WP 248 del GT29 introduce hasta nueve[7] 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 incluye algunos ejemplos de aplicación de estos criterios para determinar si la EIPD es obligatoria.

En relación con el concepto de "tratamiento a gran escala" nos resultará de utilidad otro documento publicado por el GT29, el WP 243[8] (rev.01), «Directrices sobre los delegados de protección de datos», dado que la característica "a gran escala" del tratamiento también puede resultar determinante para concretar la obligación de designar un delegado de protección de datos.

Continuando con la descripción de las circunstancias que obligan a hacer la evaluación de impacto, el Reglamento también establece que las autoridades de supervisión están obligadas a elaborar y publicar una lista con los tipos de operaciones de tratamiento que están sujetos a la exigencia de llevar a cabo una EIPD[9]. El GT29, en el WP 248, hace notar que los criterios de determinación de alto riesgo que propone también pueden servir de orientación a las autoridades de supervisión para elaborar estas listas, que se tienen que comunicar al Comité Europeo de Protección de Datos.

Con carácter potestativo, las autoridades de protección de datos también pueden elaborar y hacer pública la lista de los tipos de operaciones de tratamiento para los cuales no se debe hacer la evaluación de impacto de protección de datos. Esta lista se tiene que comunicar al Comité Europeo de Protección de Datos.

En los casos en que no esté claro si la EIPD es obligatoria, el GT29 recomienda hacerla, puesto que en cualquier caso la evaluación de impacto es una herramienta útil y práctica para ayudar a los responsables de tratamientos a cumplir con la normativa de protección de datos.

Hay algunos supuestos de tratamiento para los cuales el Grupo del artículo 29 ya determina que no hay que llevar a cabo la EIPD. Así lo considera cuando la naturaleza, el alcance, el contexto y las finalidades del tratamiento son muy similares a

[7] En la versión del WP 248 publicada en abril eran 10 criterios; en la revisión de octubre desaparecen las transferencias internacionales como un criterio que potencialmente puede llevar a considerar que el tratamiento genera de manera inherente un alto riesgo

[8] Disponible en http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[9] La autoridad Belga de protección de datos tiene publicado un proyecto de recomendación sobre las evaluaciones de impacto que incluye en su anexo 2 una lista de los tipos de operaciones para las que sería obligatorio la EIPD y en el anexo 3 una lista de tipoS de operaciones para las que no sería obligatoria (ref .: CO-AR-2016-004)

las de un tratamiento para el cual ya se ha hecho una evaluación, o cuando el tratamiento tiene como base jurídica el derecho de la Unión Europea o el de un estado miembro y la EIPD ya se ha hecho en este contexto. En ambos casos se debe argumentar sólidamente que, efectivamente, nos encontramos ante un tratamiento que encaja claramente en estas circunstancias.

En todo caso, cuando el responsable del tratamiento considere que el tratamiento no requiere hacer una EIPD, deberá justificar y documentar los motivos, incluyendo la opinión del delegado de protección de datos[10].

¿Quién está obligado a hacer la EIPD?

La obligación de hacer una EIPD afecta exclusivamente al responsable del tratamiento, sin perjuicio de que, en su caso, obtenga el apoyo y la colaboración del encargado del tratamiento y, en el caso de estar designado, del delegado de protección de datos.

Materialmente, se puede efectuar de manera interna o externa, pero hay que insistir que en ningún caso desplaza al responsable del tratamiento como sujeto obligado a la ejecución; es su obligación y, por lo tanto, debe asumir la responsabilidad de que se lleve a cabo cuando corresponda, que se haga de la manera adecuada y con los recursos necesarios y que, al final, se implanten las medidas resultantes de la evaluación, tal y como se han definido en la EIPD.

Se puede dar la circunstancia de que una misma evaluación alcance más de un proyecto de tratamiento, y que esto implique la concurrencia de varios responsables. En este caso, hay que definir la responsabilidad respecto de la EIPD de acuerdo con la intervención que cada responsable tiene en las diferentes operaciones de tratamiento.

Para hacer la EIPD, puede ser necesario que concurran toda una serie de agentes internos o externos a la organización, como pueden ser unidades o áreas específicas, expertos independientes, responsables de seguridad, áreas de tecnologías de la información e incluso, como veremos, los colectivos afectados por las operaciones de tratamiento.

[10] Incorporado en la versión 2.0 de esta guía

Es obligación del responsable del tratamiento llevar a cabo la EIPD. El GT29, en el WP 248, expresa que el responsable del tratamiento siempre responde el última instancia de la EIPD.

¿Cuál tiene que ser el contenido mínimo de una EIPD?

El resultado final de una evaluación de impacto no deja de ser un informe, o un conjunto de documentación, que recoge las características del tratamiento evaluado y las decisiones tomadas para mitigar sus riesgos, de acuerdo con su identificación, análisis, valoración y tratamiento (gestión de riesgos) y una vez analizadas, también, cuestiones como el interés legítimo (si procede), o la valoración de la necesidad y la proporcionalidad de las operaciones de tratamiento.

El artículo 35.7 del RGPD concreta cuál debe ser el contenido mínimo de la evaluación o, si se prefiere, determina qué cuestiones se tienen que analizar, como mínimo, para considerar que se ha hecho la evaluación de manera adecuada.

Una de las cuestiones que se debe abordar es captar la opinión de las personas interesadas. El RGPD, en el artículo 35.9, establece que cuando proceda el responsable del tratamiento tiene que pedir las opiniones de los interesados o de sus representantes (por ejemplo, asociaciones u otras entidades que agrupen intereses) en relación con el tratamiento que pretende llevar a cabo.

Estas opiniones se pueden obtener por varios medios, según las circunstancias en que se desarrolla el tratamiento y los colectivos afectados; si las decisiones adoptadas finalmente por el responsable del tratamiento difieren de las opiniones de las personas consultadas, conviene tener muy bien argumentadas estas decisiones.

Según el GT29, se debe documentar y argumentar, si procede, los motivos para no solicitar esta opinión. Por lo tanto, resulta más apropiado que el responsable del tratamiento se haga la pregunta de "¿Por qué no tengo que hacer la consulta?", en vez de "¿Por qué tengo que hacer la consulta?".

Si a los tratamientos evaluados se les aplica un código de conducta, su cumplimiento también debe ser objeto de la evaluación, en tanto el código incluya previsiones sobre las evaluaciones de impacto.

A pesar de que no es obligatorio, el responsable del tratamiento puede decidir publicar totalmente o parcialmente la EIPD. Esto puede generar más confianza en el proyecto y sirve al principio de "responsabilidad proactiva" y al de transparencia del tratamiento; obviamente, esta publicación no ha de generar riesgos para el tratamiento, de forma que, por ejemplo, no se tiene que publicar información relacionada con la seguridad de los datos.

Publicar la EIPD resulta de especial relevancia cuando el interés del tratamiento puede llegar a suponer un cierto impacto social o puede generar un estado de opinión en las personas los datos de las cuales pueden llegar a ser objeto de tratamiento. Los tratamientos responsabilidad de las administraciones públicas pueden generar este interés a menudo.

El tratamiento evaluado puede afectar sólo a personas de la propia organización, por ejemplo a los empleados; también en este supuesto puede ser conveniente consultarlos como parte afectadas[11].

Resulta recomendable la práctica de llevar un registro de las evaluaciones de impacto realizadas, que puede ser específico, o puede ser una información a incorporar en el registro de actividades de tratamiento, previsto en el artículo 30 del RGPD[12].

La documentación relacionada con las evaluaciones de impacto debe estar a disposición de las autoridades de supervisión, es decir, no sólo el informe final, sino también el conjunto de documentos de trabajo que se han utilizado para hacer la evaluación y que sustentan las decisiones tomadas.

¿Según el RGPD, cuál es el papel del delegado de protección de datos respecto de las EIPD?

En primer lugar, hay que decir que el RGPD determina que cuando el responsable del tratamiento debe llevar a cabo una EIPD tiene que buscar el asesoramiento del delegado de protección de datos. Este apoyo lo podemos entender tanto como una intervención activa en el diseño y ejecución de la evaluación, con funciones de

[11] Incorporado en la versión 2.0 de esta guía
[12] Incorporado en la versión 2.0 de esta guía

coordinación o de interlocución principal con los evaluadores, o bien de colaboración con el evaluador, si resulta que no tiene que asumir un papel principal en la EIPD. En este caso, queda como persona de contacto relevante dentro de la organización y tiene que atender las consultas y dar el apoyo que el responsable del tratamiento determine en cada caso.

Cuando el RGPD describe las funciones que, como mínimo, tiene que desarrollar el delegado de protección de datos, hace referencia también a la supervisión que necesariamente tiene que ejercer respecto de la correcta aplicación del resultado de la evaluación; es decir, la verificación tanto de la adecuada ejecución de la EIPD[13], como de la adecuada implantación de las medidas (decisiones) resultantes de la AIPD.

A menudo, puede haber sido el mismo delegado de protección de datos quién haya definido cómo se deben ejecutar las EIPD en la organización (por ejemplo, mediante la elaboración de una guía interna de evaluación o adoptando una guía externa que sirva de marco de evaluación); y, así mismo, quien ejecute la evaluación. En cualquier caso, es una cuestión vinculada a cómo se ha definido la gestión de la protección de datos en cada organización (establecimiento y distribución de funciones y responsabilidades), que no debe generar ningún conflicto de intereses derivado del hecho de que la evaluación y la supervisión recaigan en una misma persona. Esta decisión forma parte de la adopción de medidas que el responsable del tratamiento tiene que tomar teniendo en cuenta los riesgos.

El RGPD especifica que cuando el responsable del tratamiento debe llevar a cabo una EIPD tiene que buscar el asesoramiento del delegado de protección de datos.

El delegado de protección de datos debe controlar directa o indirectamente la ejecución de la EIPD.

[13] Incorporado en la versión 2.0 de esta guía

¿Qué consecuencias puede tener no hacer la EIPD, o no hacerla de la manera adecuada?

Si la EIPD es obligatoria y no se ejecuta, o se hace de una manera inadecuada o insuficiente, los tratamientos quedan expuestos a unos riesgos no detectados. No se habrán analizado ni valorado y, en consecuencia, no se habrán adoptado las medidas que deberían servir para mitigar los efectos negativos que las operaciones de tratamiento pueden tener para los derechos y las libertades de las personas.

Si se producen impactos negativos, esto puede suponer que el responsable o, si procede, el encargado del tratamiento cometan varias infracciones (por ejemplo: incumplimiento de obligaciones o vulneración de principios, o no atender adecuadamente derechos de las personas afectadas). Así mismo, es probable que se lleguen a producir daños y perjuicios materiales o inmateriales, algunos irreparables, para las personas afectadas; en cualquier caso, la magnitud del perjuicio y el tipo infractor a aplicar dependen de cada caso.

El art. 83.4, letra a, del RGPD, prevé como infracción no cumplir con las obligaciones previstas en los artículos 35 y 36 del RGPD.

¿Qué se debe hacer si, una vez realizada la evaluación de impacto, llegamos a la conclusión que las operaciones de tratamiento previstas continúan suponiendo un alto riesgo?

El artículo 36 del RGPD regula las denominadas "consultas previas", una obligación que recae sobre el responsable del tratamiento y que consiste en hacer una consulta a la autoridad de supervisión, antes de iniciar un tratamiento, en el caso de que a raíz de la evaluación de impacto relativa a la protección de los datos, se llegue a la conclusión de que el tratamiento comportaría un alto riesgo, por el hecho de que el responsable del tratamiento no ha sido capaz de encontrar o incorporar medidas suficientemente efectivas como para mantener controlados los riesgos en un nivel aceptable; estaremos en la situación que el riesgo residual, el que queda después de haber previsto aplicar medidas para mitigar el riesgo inherente, continúa suponiendo un

riesgo inaceptable para los derechos y las libertades de las personas, cuyos datos se ha previsto que sean objeto de tratamiento.

El procedimiento de consulta previa implica que, en un plazo de ocho semanas desde que se ha solicitado, la autoridad de supervisión debe contestar la consulta por escrito; existe la posibilidad de ampliar este plazo seis semanas más, de acuerdo con la complejidad del tratamiento sujeto a consulta previa. Estos plazos se pueden suspender hasta que la autoridad disponga de toda la información necesaria para responder la consulta (art. 36.2 del RGPD).

La autoridad de protección de datos, en el contexto de una consulta previa, puede utilizar cualquiera de los poderes recogidos al artículo 58 del RGPD, tanto los de investigación como los correctivos, como por ejemplo «imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición» (art. 58.2.f del RGPD).

Al hacer la consulta previa, el responsable del tratamiento debe facilitar a la autoridad de control la información siguiente:

- Si procede, las responsabilidades del responsable, los corresponsables y los encargados implicados en el tratamiento, especialmente en caso del tratamiento efectuado dentro de un grupo empresarial.
- Las finalidades y los medios del tratamiento previsto.
- Las medidas y garantías que, en conformidad con el RGPD, se han previsto para proteger los derechos y las libertades de los interesados.
- Si procede, los datos de contacto del delegado de protección de datos.
- La evaluación de impacto relativa a la protección de datos establecida en el artículo 35.
- Cualquier otra información que solicite la autoridad de control.

Como ya se ha mencionado, siempre debe conservarse la documentación que acredita que se ha llevado a cabo la EIPD, con independencia de que el responsable del tratamiento haya tenido que hacer, o no, la consulta previa. Esa conservación es conveniente articularla a partir de un registro interno de evaluaciones de impacto, o a partir del registro de actividades de tratamiento.

Revisión de la evaluación de impacto

El tratamiento de datos personales en su conjunto, o bien cada una de las operaciones de procesamiento de la información que conforman un tratamiento, pueden variar a lo largo del tiempo. Estos cambios en relación con la situación inicial de los tratamientos pueden afectar a los riesgos o a las medidas previstas para mitigar los riesgos y, por eso, se deben prever mecanismos de revisión de las evaluaciones.

El RGPD establece que el responsable del tratamiento debe revisar la vigencia de la evaluación inicial cuando se produzcan cambios relevantes en los tratamientos, especialmente si estos cambios pueden implicar una variación de los riesgos detectados o de las medidas adoptadas, como por ejemplo: recogida de nuevos tipos de datos, migración de plataformas tecnológicas, nuevas aplicaciones, cambios en las medidas de seguridad, un tiempo superior de retención de los datos, cambios normativos, etc.

Las evaluaciones de impacto en la Directiva (UE) 2016/680

La Directiva 2016/680, relativa a la protección de las personas físicas en cuanto al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, formó parte del paquete de protección de datos junto con el RGPD. Ambos textos se aprobaron al mismo tiempo.

La Directiva 2016/680, que se tiene que transponer como máximo el 6 de mayo de 2018, establece las directrices sobre transmisión de datos por cuestiones judiciales y policiales. Esta directiva será de aplicación en el intercambio de datos transfronterizo dentro de la UE y establece también unos estándares mínimos para el tratamiento de datos en cada estado de la Unión Europea.

La finalidad de la Directiva es proteger a todas las personas implicadas en investigaciones policiales o procesos judiciales, ya sea en condición de víctimas, acusados o testigos, clarificando sus derechos y estableciendo límites en la transmisión de los datos relacionados con la prevención, investigación, detección y enjuiciamiento de delitos o la imposición de penas. También incluye salvaguardas para

evitar riesgos para la seguridad pública, y se orienta a facilitar una cooperación más rápida y efectiva entre las autoridades policiales y judiciales de los estados miembros.

Así mismo, el artículo 27 prevé que los tratamientos en los cuales es de aplicación la Directiva también pueden ser objeto de una EIPD, y establece unas circunstancias equivalentes a las que prevé el RGPD[14]. Lo mismo sucede con el contenido mínimo de la EIPD, regulado en el artículo 27.2 de la Directiva, que sería equivalente al artículo 35.7 del RGPD.

En consecuencia, de acuerdo con la transposición que se haga de esta Directiva, cada legislación nacional regulará la obligación de llevar a cabo la EIPD en los tratamientos relacionados con la transmisión de datos de carácter personal a los que aplica la Directiva.

Por la forma en que se recoge en la Directiva, el método de evaluación a utilizar podría ser el mismo que para los tratamientos de datos personales regulados por el RGPD.

El artículo 28 regula la consulta previa, que ya hemos analizado desde la perspectiva del RGPD. En esta cuestión la regulación también es equivalente, excepto en alguna cuestión específica, como el hecho que las listas que pueden elaborar las autoridades de control tienen que determinar, no qué tratamientos tienen que ser objeto de evaluación (caso del RGPD), sino qué tratamientos deberán ser objeto de consulta previa. Es decir, con independencia del resultado de la evaluación, habrá casos en que la consulta previa será obligatoria antes de iniciar el tratamiento de los datos.

[14] Articulo 35.1 del RGPD

PARTE 2

Orientaciones para la ejecución de la evaluación de impacto

ASPECTOS PREPARATORIOS DE LA EJECUCIÓN DE LA EVALUACIÓN DE IMPACTO

La evaluación de impacto relativa a la protección de datos es un conjunto de actividades que tienen una finalidad concreta. En este sentido, se deben prever qué recursos se dedicarán (equipo de trabajo), cuando y de qué manera se llevará a cabo (planificación y método), qué documentación se generará o se utilizará (gestión documental) y cómo se entregarán los resultados (informe de evaluación); en definitiva, se debe organizar como se llevará a cabo la evaluación[15].

Tal como se ha dicho, 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.

El método de trabajo que propone esta guía para hacer evaluaciones de impacto se estructura en seis fases que se muestran a continuación, cada una de las cuales comporta una serie de actividades que se describen, en forma de orientaciones, a lo largo de esta guía.

[15] Respecto de las cuestiones organizativas de ejecución de la evaluación de impacto, resulta útil tener en cuenta lo que prevé la ISO/IEC 29134:2017 en su apartado "6.3 Preparation of the PIA"

Entre las actividades preparatorias, debemos tener muy en cuenta la necesidad de identificar de manera clara los diferentes interlocutores que nos tienen que proporcionar información para ejecutar la EIPD o que tienen que validar los progresos que hacemos, como sucede en cualquier otro tipo de proyecto. El responsable del tratamiento, junto con las personas que pueden ejercer funciones de seguridad, de delegado de protección de datos, de responsables de áreas funcionales implicadas o de tecnologías, son algunos de los perfiles que se deben tener en cuenta en el momento de obtener esta información; incluso, según las particularidades del proyecto que se tiene que evaluar, puede ser necesario recurrir a profesionales de disciplinas diversas: sociólogos, médicos, asistentes sociales, educadores, matemáticos, abogados, etc.

Estos colectivos pueden proporcionar información muy relevante, no sólo de los aspectos funcionales y tecnológicos del proyecto, también respecto de la identificación y análisis de los riesgos, e incluso pueden participar en la estimación del nivel de riesgo[16].

Identificar de manera clara los diferentes interlocutores que nos tienen que proporcionar información para ejecutar la EIPD o que tienen que validar los progresos que hacemos.

Cuando el WP 248, en el apartado dedicado a definir algunas directrices para ejecutar la EIPD, se plantea "¿Quién está obligado a hacer la EIPD?", hace referencia a que es una buena práctica definir y documentar los roles y las responsabilidades específicas en el marco de la EIPD, y pone varios ejemplos:

- Cuando hay unidades de negocio específicas del responsable del tratamiento que proponen hacer una EIPD, estas unidades tienen que aportar información esencial para ejecutar la evaluación y tienen que participar en el proceso de validación.

- Si procede, se recomienda consultar a expertos independientes de ámbitos profesionales diversos.

[16] Incorporado en la versión 2.0 de esta guía

- Se tiene que contar con la ayuda del encargado del tratamiento. A pesar de que la casuística puede ser muy diversa, el caso más claro pero seguramente menos común sería hacer participar al encargado del tratamiento en la EIPD. Es muy probable que, en el futuro, este apoyo del encargado del tratamiento se materialice mediante las EIPD que el mismo encargado puede hacer de los tratamientos de datos relacionados con los servicios que presta[17]. Esta EIPD del encargado no tiene que implicar que el responsable del tratamiento deje de hacer su propia evaluación de impacto, puesto que la EIPD del encargado tendrá un carácter muy genérico, enfocado a sus servicios, y por lo tanto el responsable de tratamiento tendrá que adaptarla a las operaciones concretas que tiene previsto llevar a cabo.

- El delegado de protección de datos puede plantear al responsable del tratamiento la necesidad de hacer la EIPD de un tratamiento o de operaciones de tratamiento concretas, y tendría que dar el apoyo metodológico necesario (selección de la metodología o, incluso, aportar una guía de evaluación propia de la organización). Así mismo, tiene que valorar si la gestión del riesgo está ajustada a las características de los riesgos del tratamiento y ayudar a determinar si el riesgo residual es aceptable. Obviamente, además, tiene que contribuir a que el responsable del tratamiento tome conciencia del contexto en el cual está desarrollando las actividades de tratamiento y, en otro plan, tiene que supervisar que la implantación de los resultados de la EIPD sea adecuada.

- El responsable de seguridad de la información, si hay, o el departamento de tecnologías de la información, tienen que proporcionar asistencia al responsable del tratamiento. También pueden proponer hacer una EIPD de una operación específica de tratamiento, de acuerdo con las necesidades tecnológicas y operativas, o de seguridad, que se puedan derivar.

En todo caso, siempre se debe tener en cuenta que el destinatario del resultado de la evaluación es el responsable del tratamiento, que es quien tiene que tomar las decisiones sobre los riesgos detectados y proponer las medidas para mitigarlos, de acuerdo con la evaluación de impacto.

[17] A pesar de no estar obligados, es muy probable que los encargados de tratamientos utilicen estas evaluaciones como un valor añadido de sus servicios en clave competitiva.

No entraremos aquí en la parte de organización del proyecto de evaluación, puesto que esta guía no está dirigida a la gestión de proyectos. Por consiguiente, si la organización ya tiene un sistema de gestión de proyectos, lo puede aplicar al proceso de evaluación.

A continuación, se enumeran los aspectos preparatorios u organizativos más relevantes y que se deberían tener en cuenta, como mínimo:

- Evidentemente, el responsable del tratamiento debe saber que se iniciará un proceso de evaluación de impacto, puesto que a partir de la evaluación se harán propuestas para reducir los riesgos. A raíz de estas propuestas el responsable tendrá que tomar decisiones, como por ejemplo priorizar la aplicación de las medidas propuestas o asignar recursos humanos y materiales.

- Se debe tener claro qué método de evaluación seguiremos, es decir, qué guía o qué pautas de trabajo utilizaremos para hacer la evaluación, que es un aspecto especialmente relevante para que el proceso sea sistemático (especialmente en su dimensión de repetible). Puede ser una guía estándar, una guía interna o unas simples pautas, elaboradas por la misma organización.

- Se deben tener identificados claramente los diferentes interlocutores que participarán en el proceso de evaluación, especialmente el delegado de protección de datos –si está designado- o la figura equivalente. Cómo hemos visto, el RGPD le asigna algunas funciones concretas en relación con las EIPD.

- Se debe considerar si el equipo de evaluación tiene que ser externo o interno. Se deben tener en cuenta, por ejemplo, posibles relaciones contractuales para regular la actividad del evaluador (si es externo), o aspectos relacionados con descripciones de puestos de trabajo y posición dentro de la organización (si es interno).

Conviene que al menos estas cuatro cuestiones estén bien definidas antes de iniciar el proceso de evaluación, aparte que los métodos de trabajo de la organización y de gestión de proyectos prevean otras cuestiones adicionales.

Como paso previo a la EIPD, es habitual que las guías de evaluación de impacto planteen analizar si la evaluación es necesaria, es decir, debemos preguntarnos: «¿Estamos obligados a llevar a cabo una evaluación de impacto relativa a la protección de datos?» [18].

Y, obviamente, debemos responder esta pregunta con argumentos, que tienen que quedar documentados tanto si la respuesta es positiva cómo si es negativa; lo podemos considerar como un paso previo a la ejecución de la EIPD. A continuación, se orienta sobre como determinar la obligación de hacer la EIPD.

[18] Como ya se ha mencionado el proyecto de LOPD lo prevé como una obligación.

ANÁLISIS DE LA NECESIDAD DE HACER LA EVALUACIÓN DE IMPACTO

Todo y que pueda resultar evidente, lo primero que debemos hacer es analizar si la iniciativa implica el tratamiento de datos de carácter personal sujetos al marco jurídico que regula el derecho a la protección de los datos de carácter personal, qué tipo de datos se ha previsto recoger o tratar y a qué operaciones de tratamiento se someterán[19].

A priori, determinar si se prevé tratar datos de carácter personal no tendría que implicar una dificultad extraordinaria, puesto que si se está iniciando un proceso de evaluación de impacto es porque ya se ha identificado que el nuevo proyecto o iniciativa implica el uso de datos personales. En cualquier caso, se debe disponer de la siguiente información sobre el tratamiento que estamos analizando:

- ¿Qué datos se tratarán, y de quién? Tenemos que elaborar una "lista" exhaustiva de todos los datos que pueden ser objeto de las diferentes operaciones de tratamiento, por ejemplo: nombre, apellidos, fecha de nacimiento, número de teléfono móvil, dirección postal completa, dirección de correo electrónico, imagen, datos biométricos, datos relativos a la salud, datos calculados, etc.

  En cuanto a los datos, también se debe hacer una aproximación del volumen de personas afectadas por el tratamiento o si estamos recogiendo muchos tipos de datos diferentes, esto resultará útil posteriormente, en el momento de determinar si es un tratamiento "a gran escala" o no.

  Por último, también se debe saber si se prevé tratar datos de niños, de personas en situación de vulnerabilidad o en otras circunstancias que puedan evidenciar situaciones especiales que requieren que los datos de carácter personal se traten con especial cautela. Así mismo, conviene tener en cuenta si el tratamiento de estos datos puede ser incidental.

[19] En este sentido hay que tener en cuenta los artículos 2 y 3 del RGPD, que regulan el ámbito material y territorial de aplicación del Reglamento, respectivamente

- ¿Qué se prevé hacer con los datos? Se debe identificar a qué operaciones de tratamiento se prevé someter a los datos: recogida, almacenamiento, anonimización o seudoanonimización, consulta, modificación, supresión, etc., y qué tecnologías o medios se utilizarán para tratarlas (es suficiente una identificación resumida de las tecnologías, poniendo especial atención a las que puedan resultar más invasivas para la intimidad, o que podamos considerar tecnologías emergentes).

A título recordatorio, hay que tener presente que el RGPD define:

- Tratamiento: cualquier operación o conjunto de operaciones que se aplican a unos datos de carácter personal, de manera automatizada o no, es decir:
  - recogida
  - registro
  - organización
  - estructuración
  - almacenamiento
  - adaptación o modificación
  - extracción
  - consulta
  - utilización
  - comunicación por transmisión, difusión o cualquiera otro medio disponible
  - comparación o combinación
  - restricción
  - supresión
  - destrucción

- Datos personales: cualquier información sobre una persona física identificada o identificable («el interesado»); se considera persona física identificable cualquier persona de la cual se pueda determinar la identidad, directamente o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de la persona.

En relación con el concepto de dato personal, conviene tener en cuenta otras definiciones recogidas en el artículo 4 del RGPD:

- Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física, que proporcionen una información única sobre la fisiología o la salud de esta persona, obtenidas del análisis de una muestra biológica.

- Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, que permiten o confirman la identificación única de esta persona, como imágenes faciales o datos dactiloscópicos.

- Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Y en relación con los tipos de datos de carácter personal, se debe tener muy en cuenta si el tratamiento afecta las denominadas "categorías especiales de datos personales" que se describen en el artículo 9 del RGPD, o a los datos descritos en el artículo 10, que incluyen las que pueden revelar:

- el origen étnico o racial
- las opiniones políticas
- las convicciones religiosas o filosóficas
- la afiliación sindical
- los datos genéticos
- los datos biométricos dirigidos a identificar de manera unívoca una persona física
- los datos relativos a la salud
- los datos relativos a la vida sexual o las orientaciones sexuales
- los datos relativos a condenas e infracciones penales o medidas conexas[20]

Tenemos que documentar la información recogida para responder a las preguntas “¿qué datos se ha previsto tratar?” y “¿que se hará con los datos?”, puesto que esta

[20] Incorporado en la versión 2.0 de esta guía

información la tendremos que incorporar posteriormente al informe de análisis de necesidad o, si procede, al apartado del análisis de la necesidad del informe de evaluación de impacto.

En la parte 3 de esta guía se proporcionan varios modelos de documentos y plantillas, que se aportan como orientación de los diversos documentos a elaborar, ya sean de trabajo o para entregar como documentos finales; todos estos modelos se aportan como una primera ayuda y, por lo tanto, se pueden modificar y adaptar. Se incluye un conjunto de plantillas orientadas a recoger y clasificar la información necesaria para decidir sobre la obligación de hacer la EIPD (véase modelo 1[21]).

Si finalmente no se hacen operaciones de tratamiento de datos de carácter personal, el RGPD no se aplica y, por consiguiente, no hay que llevar a cabo la EIPD. Esta decisión se tiene que argumentar mediante un informe que detalle en qué se fundamenta esta conclusión; no tiene que ser un informe "aislado", sino que se debe situar en el contexto de la etapa previa a una EIPD[22], puesto que puede ser necesario justificar la decisión ante la autoridad de supervisión competente.

Si se llega a la conclusión de que se tratan datos de carácter personal sujetos a la normativa de protección de datos, se tiene que pasar a valorar si en el tratamiento concurren algunas de las circunstancias o situaciones que obligan a hacer la EIPD.

Ya sabemos que, con carácter general, se debe ejecutar la evaluación de impacto cuando un tratamiento puede suponer un alto riesgo para los derechos y las libertades de las personas físicas, especialmente (pero no exclusivamente) si se utilizan nuevas tecnologías y teniendo en cuenta la naturaleza, alcance, contexto o finalidades del tratamiento (considerando 76 y art. 35.1 del RGPD).

En cuanto a la estimación del nivel de riesgo, el Reglamento considera que este debe ponderarse mediante una evaluación objetiva que determine si las operaciones de tratamiento de datos comportan riesgo, o si el riesgo es alto.

Hay una serie de características de las operaciones de tratamiento que pueden inducirnos a pensar que hay un riesgo "significativo" para los derechos y las libertades.

[21] Este modelo se ha simplificado en la versión 2.0 de esta guía

[22] Hay que recordar que el proyecto de LOPD prevé que este análisis previo sea una obligación

Precisamente esta primera aproximación al grado de riesgo es lo que tenemos que hacer en esta etapa previa, sin hacer todavía una valoración formal o cuantitativa del nivel de riesgo.

En una primera aproximación muy simple, podemos definir el riesgo como la proximidad de un posible daño y, intuitivamente, calificaremos una situación “de alto riesgo" cuando este daño potencial puede ser muy grave. Por tanto, la potencial gravedad de las consecuencias que se puedan derivar de un tratamiento serán determinantes para concluir que nos encontramos ante una situación de mucho riesgo, es decir, de un riesgo alto.

Existe un parámetro que, a todos los efectos, se debe considerar en el momento de valorar el riesgo: la probabilidad de que este daño se llegue a producir. Este segundo parámetro (probabilidad), todo y que podemos tenerlo presente, no lo utilizaremos en esta fase previa de análisis de la necesidad de la EIPD, sino que lo utilizaremos cuando llevemos a cabo la gestión riesgos de una manera más cuantitativa.

Situados en el contexto de las EIPD, tenemos que considerar que hay un alto riesgo cuando las operaciones de tratamiento de los datos personales pueden causar una vulneración grave de los derechos y las libertades de las personas de las cuales se tratan los datos.

Por derechos y libertades tenemos que entender todos los reconocidos como fundamentales por el ordenamiento jurídico, incluidos los reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea, en la cual también se reconoce el derecho a la protección de los datos de carácter personal (art. 8 de la Carta).

¿Cuándo podemos considerar, con carácter general, que se puede producir una vulneración grave de los derechos y las libertades fundamentales? El RGPD hace referencia a:

- Cuando el tratamiento de los datos personales pueda llegar a impedir el libre ejercicio de los derechos y las libertades a sus titulares.
- Cuando el tratamiento de los datos personales pueda dejar sin contenido el derecho o la libertad.

- Cuando el tratamiento de los datos personales pueda ser el origen de «daños y perjuicios físicos, materiales o inmateriales» para las personas interesadas.

En el WP 248, el GT29 aporta una serie de criterios que sirven para detectar si un tratamiento comporta, de manera inherente, un elevado riesgo potencial, o un riesgo significativo. Se debe recordar que, en este mismo documento, el GT29 deja claro que el RGPD no requiere que se haga una EIPD para cada tratamiento del cual se deriven riesgos para los derechos y las libertades de las personas, sino que sólo es obligatoria cuando puede dar lugar a un alto riesgo.

A continuación, se relacionan los criterios mencionados. Para una descripción más amplia, debemos acudir al WP 248[23].

- Evaluación o "puntuación" de personas, incluida la elaboración de perfiles y la predicción de conductas o comportamientos.
- Toma automatizada de decisiones con efecto jurídico o similar significativo.
- Observación sistemática.
- Datos sensibles, o datos muy personales[24], que incluye las categorías especiales de datos tal como se definen al artículo 9 del RGPD, así como los datos personales relativos a condenas e infracciones penales (art. 10 RGPD).
- Tratamientos de datos a gran escala: el RGPD no define qué constituye a gran escala; más adelante, en esta guía se proporcionan algunas orientaciones[25].
- Asociación o combinación de conjuntos de datos que puedan exceder las expectativas razonables de las personas interesadas[26].
- Datos relativos a sujetos vulnerables (considerando 75).
- Utilización innovadora o aplicación de nuevas soluciones tecnológicas u organizativas.
- Cuando el tratamiento impide a las personas afectadas ejercer un derecho o utilizar un servicio o ejecutar un contrato (art. 22 y considerando 91).

[23] En la primera versión del WP 248, publicada en abril de 2016, la transferencia de datos fuera de la Unión Europea (considerando 116) también era un criterio para detectar el alto riesgo
[24] Incorporado en la versión 2.0 de esta guía
[25] Las que prevé el WP 243 del GT29 sobre el delegado de protección de datos
[26] Hay que tener presente el WP 203 del GT29 sobre la limitación de la finalidad (página 24)

El GT29, en el WP 248, considera que cuanto más de estos criterios cumpla un tratamiento, u operaciones concretas de tratamiento, más probable es que concurra un alto riesgo para los derechos y las libertades de los interesados.

El WP 248 establece una orientación de carácter general: en los tratamientos en que concurren dos o más criterios el responsable del tratamiento puede considerar que hay que hacer la EIPD, ya que las operaciones de tratamiento probablemente supongan un alto riesgo. Ahora bien, la orientación de cumplir con más de un criterio se tiene que tomar como una simple orientación, puesto que es posible que, en razón de otros factores, el responsable del tratamiento también puede considerar que debe hacerse la EIPD, aunque para ese tratamiento solo concurra uno de esos criterios.

Tampoco se puede descartar que el responsable del tratamiento considere que, a pesar de que las operaciones de tratamiento cumplen al menos dos criterios, potencialmente del tratamiento no se deriva un alto riesgo. En ese caso, se deben documentar y argumentar las razones por las cuales no se hace la EIPD e identificarlas con claridad, incorporando la opinión del delegado de protección de datos[27] (en el caso de que esté designado).

En conjunto, tenemos que disponer de la información necesaria sobre las características básicas del tratamiento, para analizar si implica cualitativamente un alto riesgo para los derechos y las libertades de las personas. Este análisis se tiene que sustentar en lo que prevé el artículo 35 del RGPD, que recoge una serie de supuestos tasados en qué es obligatorio hacer la EIPD.

Para determinar la obligatoriedad de llevar a cabo la evaluación, se pueden plantear hasta tres niveles de análisis.

Primer nivel de análisis

El primer nivel de análisis consiste en verificar si el tratamiento está incluido en alguna de las listas previstas a los artículos 35.4 y 35.5 del RGPD.

Por lo tanto, cuando estas listas estén disponibles, primero tendremos que verificar si el tratamiento del cual tenemos que determinar la necesidad de hacer la evaluación de

[27] Incorporado en la versión 2.0 de esta guía

impacto se incluye en los tipos de tratamiento que no requieren la EIPD (art. 35.5). Si aparece claramente en esta lista, ya podemos elaborar el informe que determina que no hay que hacerla. Ahora bien, hace falta que nos aseguremos que efectivamente el tratamiento encaja, sin lugar a dudas, en los tipos de tratamiento para los cuales la autoridad de protección de datos ha decidido que no hay que hacer la EIPD; si tenemos dudas, lo más prudente es consultar a la autoridad de control competente.

Si el tratamiento no aparece en la lista de los excluidos, se debe verificar si está incluido en la lista de los que, a juicio de la autoridad de control, sí que requieren la EIPD (art. 35.4). Si es así, se debe recoger en el informe e iniciar la EIPD.

En cuanto a esta segunda lista, se debe tener en cuenta que no es exhaustiva y que se irá actualizando[28], de forma que el hecho que nuestro tratamiento tampoco aparezca en esta lista no implica, automáticamente, que no tengamos que hacer la EIPD. Debemos, pues, pasar al segundo nivel de análisis.

Segundo nivel de análisis

El segundo nivel de análisis se centra en determinar si el tratamiento está incluido en los casos previstos en el artículo 35.3 del RGPD. A efectos prácticos, este artículo ya contiene una primera lista de tipo de tratamientos que requieren la EIPD, en este caso elaborada por el legislador europeo. Respecto de estos supuestos, sucede lo mismo que con la lista elaborada por la autoridad de control: si el tratamiento no encaja, no se puede afirmar que no debamos llevar a cabo la EIPD, sino que tenemos que recurrir a un tercer nivel de análisis para estar completamente seguros.

El artículo 35.3 recoge tres casos en qué es obligatorio hacer la EIPD:

- Cuando la finalidad es la evaluación "sistemática y exhaustiva", de carácter automatizado, de varios aspectos de la persona, en general cuando se elaboran perfiles y su alcance implica efectos de tipo jurídico, o que pueden afectar significativamente a las personas como consecuencia de la toma de decisiones basadas en la información que se trata.

[28] Obviamente la no exhaustividad y la actualización también aplica a la lista de los tratamientos que no requieren hacer EIPD

- El segundo caso se refiere a la naturaleza del tratamiento, si se pretenden tratar a gran escala categorías especiales de datos o datos personales relativos a condenas e infracciones penales (más adelante se dan algunas orientaciones respecto del concepto “a gran escala”).

- Para el tercer caso también es de aplicación la idea del tratamiento a gran escala, pero vinculado a "la observación" sistemática[29] de zonas de acceso público. Tenemos que interpretar el concepto "observación" de manera amplia, como equivalente de "seguimiento"; por lo tanto, no tiene por qué limitarse a los sistemas de videovigilancia, sino que su alcance incluye cualquier tratamiento que implique la monitorización de personas.

Si de lo que prevé el artículo 35.3 se deduce que el tratamiento tiene que ser objeto de EIPD, lo recogeremos así en el informe de evaluación de la necesidad y haremos la evaluación.

En cuanto al concepto de tratamiento a gran escala, el RGPD no proporciona una definición concreta. No obstante, el considerando 91 sí que orienta sobre el significado que puede tener, cuando se refiere a las “operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales en el ámbito regional, nacional o supranacional y que podrían afectar a un gran número de interesados”.

Por lo tanto, hay dos variables que inicialmente se tienen que valorar, en el momento de determinar si se trata de un tratamiento a gran escala:

- La diversidad de tipos de datos y la cantidad de datos que se tratan.
- El número de personas que se pueden ver afectadas por las operaciones de tratamiento.

[29] Para considerar que la observación cumple con el requisito de sistemática, conviene aplicar los criterios que recoge el WP 243 del GT29: hecho de acuerdo a un sistema; preestablecido, organizado y metódico; que tiene lugar como un plan general de recogida de datos; que se hace como parte de una estrategia

En cuanto a la concreción del concepto "a gran escala", también disponemos de unas primeras orientaciones, vinculadas a las directrices que el GT29 recoge en el WP 243 sobre el delegado de protección de datos.

De acuerdo con esas directrices, no se puede concretar un volumen preciso de datos o personas afectadas para aplicarlo de manera genérica a cualquier tratamiento; por tanto, no hay un valor cuantitativo especifico de datos o personas a partir del cual se debería considerar que estamos ante un tratamiento a gran escala. Esto, sin perjuicio que en algunos casos concretos se pueda llegar a concretar.

En el WP 243, el Grupo de trabajo del artículo 29 identifica una serie de factores que pueden indicar que se trata de un tratamiento a gran escala. No se tiene que considerar una lista cerrada, puesto que son unas orientaciones de carácter general. Así, tendríamos:

- El número de personas de las cuales se tratan los datos personales, ya sea en valores absolutos (número concreto), o un porcentaje relevante de personas de un determinado contexto o ámbito.
- El volumen de información o la gama de diferentes tipos de datos que se tratan.
- La duración, o permanencia, del tratamiento.
- La extensión geográfica del tratamiento.

Si el tratamiento se incluye en alguno de los casos descritos en el artículo 35.3, se deben incluir, las circunstancias que obligan a ejecutar la evaluación de impacto en el informe de análisis de la necesidad de hacer la EIPD.

Si el tratamiento no encaja en ninguno de los tres casos, tenemos que recurrir a un tercer nivel de análisis sobre la necesidad de llevar a cabo, o no, la evaluación de impacto.

Tercer nivel de análisis

El tercer nivel de análisis tiene un carácter más amplio o generalista. Se trata de un análisis sustentado en lo que prevé el artículo 35.1 del RGPD, de forma que se deben verificar los siguientes aspectos:

– La naturaleza del tratamiento: se trata de valorar las características esenciales del tratamiento, para verificar si puede suponer el alto riesgo a que hemos hecho referencia. Por ejemplo:
  - si de manera prioritaria se tratan categorías especiales de datos
  - si se tratan datos a gran escala
  - si se hace un seguimiento exhaustivo de personas
  - si se combinan diferentes conjuntos de datos (varias fuentes de información)
  - si los datos se refieren a personas en situación de vulnerabilidad
  - si la legitimación del tratamiento se basa en el interés legítimo
  - si los datos están destinados a ser tratados durante largos periodos de tiempo
  - cualquier otra circunstancia que forme parte intrínseca del tratamiento

– El alcance del tratamiento: se trata de valorar los efectos o consecuencias del tratamiento, hasta dónde puede llegar y si puede suponer un alto riesgo. Por ejemplo, si implica:
  - toma de decisiones con efectos jurídicos
  - toma de decisiones en procesos competitivos
  - valoración de riesgos crediticios
  - exclusión de beneficios sociales o fiscales
  - en definitiva, con independencia de la finalidad del tratamiento, qué efectos significativos, directos o indirectos, puede tener sobre las personas

– El contexto del tratamiento: se trata de valorar el conjunto de circunstancias en que se harán las operaciones de tratamiento, con objeto de verificar si pueden suponer un alto riesgo. Por ejemplo:
  - uso de nuevas tecnologías o tecnologías emergentes
  - uso de tecnologías especialmente invasivas para la privacidad
  - uso de tecnologías que de manera inherente añadan riesgos
  - varios responsables de tratamiento
  - cadenas de encargados de tratamiento complejas
  - transferencias internacionales

- cualquier otra circunstancia en la cual se llevan a cabo las operaciones de tratamiento y que puede generar un riesgo relevante para los derechos y las libertades de las personas

– Las finalidades del tratamiento: se trata de identificar cuál es la finalidad del tratamiento, y si de la finalidad se deriva un riesgo significativo. Por ejemplo, si la finalidad es:
  - la toma de decisiones
  - la elaboración de perfiles
  - el análisis predictivo
  - la prestación de servicios relacionados con la salud
  - el seguimiento, control u observación de personas
  - en definitiva, finalidades relevantes desde la perspectiva de la protección de los derechos y las libertades de las personas

En este tercer nivel de análisis, se debe tener en cuenta los criterios que el GT29 propone en el WP 248 para detectar el alto riesgo.

En la parte 3 de esta guía se incluyen unas listas de verificación que sintetizan todo este proceso de análisis (véase modelo 2), con una serie de preguntas que ayudan a determinar si se trata de un tratamiento que requiere de la evaluación de impacto.

Tenemos que considerar las evaluaciones de impacto como un instrumento avanzado de cumplimiento de la regulación del derecho de la protección de los datos de carácter personal, y tener en cuenta que el Reglamento procura no plantear cargas extraordinarias para los pequeños y medianos responsables de tratamientos. En consecuencia, en el momento de concretar ciertas obligaciones se analizan un conjunto de parámetros del tratamiento que no se centran exclusivamente en el tipo de datos tratados, como hasta ahora, sino que, por ejemplo, el volumen de datos tratados es relevante respecto de la exigencia de determinadas obligaciones.

Una vez recogida y analizada toda la información relacionada con las operaciones de tratamiento que se pretenden llevar a cabo, podemos determinar si existe obligación, o no, de hacer la EIPD.

Por lo tanto, elaboraremos un informe que tiene que determinar y argumentar si hay que hacer la evaluación de impacto, o no. En la parte 3 de esta guía se proporciona una propuesta de índice de este informe (véase modelo 3).

Otras cuestiones a tener en cuenta: las personas afectadas

En algún caso concreto se puede plantear la necesidad de consultar a las partes afectadas, ya en esta etapa previa a la evaluación de impacto, tudo y que el RGPD lo prevé solo en relación a la ejecución de la EIPD. Por tanto, conviene tener claramente identificados los colectivos de personas que se verán afectados por las operaciones de tratamiento y si, como grupo, o grupos, podemos dirigirnos a algún interlocutor válido que represente sus intereses (instituciones, sindicatos, comité de empresa, grupos de usuarios, asociaciones, organizaciones no gubernamentales, administraciones públicas de ámbitos diversos, consejo escolar, etc.).

Según cual sea la iniciativa concreta, tenemos que valorar si conviene hacerles partícipes de la reflexión que implica decidir sobre la necesidad de llevar a cabo la evaluación, así se sentirán implicados y estarán informados desde el principio, de forma que cuando se recoja su opinión (si finalmente se hace la EIPD), estarán en una posición mejor para aportarla. Se trata de hacer, en la fase de diseño del proyecto, un cierto ejercicio de transparencia respecto de las operaciones de tratamiento y del uso que se quiere dar a los datos de carácter personal.

Obviamente, la consulta a las partes o colectivos afectados se puede hacer en cualquier momento a lo largo del proceso de evaluación, y más de una vez, todo dependerá del proyecto de que se trate.

El WP 248 trata la cuestión de pedir las opiniones de los interesados o de sus representantes y considera que:

- Las opiniones se pueden obtener por varios medios, según el contexto: un estudio interno o externo relacionado con el objetivo y los medios de tratamiento, una pregunta formal a los representantes del personal o a los sindicatos o, incluso, una encuesta enviada a las personas afectadas por el tratamiento.

- Si las decisiones adoptadas finalmente por el responsable del tratamiento difieren de las opiniones de los interesados, los motivos se tienen que documentar y argumentar.

- El responsable del tratamiento también tiene que documentar la justificación de no solicitar las opiniones de los interesados, si decide que no es adecuado.

Para acabar con las orientaciones sobre esta etapa previa, que aborda la decisión sobre la necesidad de hacer la EIPD, conviene añadir que si el resultado del análisis concluye que no estamos obligados a llevar a cabo la EIPD, sería conveniente hacer una reflexión adicional sobre si, a pesar de no ser obligatoria, es recomendable hacerla debido a otros factores: la reputación respecto de los clientes o del sector, el uso como valor competitivo en el mercado, demostrar el compromiso con el cumplimiento normativo (*accountability*), la opinión pública ante un tratamiento de interés general o impacto social, el fomento de la participación ciudadana, etc.

En las conclusiones del WP 248, el GT29 considera que las EIPD son una forma útil para que los responsables de tratamientos implementen sistemas de tratamiento de datos que cumplan el RGPD. Como orientación, recomienda que cuando no está claro si la EIPD es obligatoria o no, se haga la evaluación, puesto que en cualquier caso la EIPD es un instrumento que ayuda a cumplir el RGPD.

Las políticas de protección de datos de los responsables de tratamientos pueden incluir declaraciones respecto de los tratamientos que serán objeto de evaluación de impacto, ampliando los supuestos previstos en la regulación[30].

[30] Incorporado en la versión 2.0 de esta guía

DESCRIPCIÓN SISTEMÁTICA DE LAS OPERACIONES DE TRATAMIENTO

Una vez hemos determinado que la EIPD es obligatoria, es imprescindible conocer con detalle qué datos concretos se tratarán, qué operaciones de tratamiento se pretenden hacer y en qué circunstancias, por tanto hay que disponer de un conocimiento preciso de los mismos, que permita afrontar la gestión de los riesgos que potencialmente puedan presentar los tratamientos.

Una buena parte de la información que utilizaremos ahora ya se ha recogido y analizado durante la etapa previa, es decir, cuando hemos valorado la necesidad de hacer la evaluación; recordemos que ya tenemos información sobre los datos involucrados en el tratamiento y sobre las operaciones de tratamiento que se ha previsto llevar a cabo. Está información deberá reutilizarse durante el proceso de evaluación de impacto.

El artículo 35.7.a del RGPD obliga a que la evaluación de impacto incluya, como mínimo, una descripción sistemática de las operaciones de tratamiento previstas y de las finalidades del tratamiento y, si procede, el interés legítimo perseguido por el responsable del tratamiento. En esta parte de la guía, nos centraremos en elaborar un documento que recoja con detalle la descripción del tratamiento (proyecto) y del conjunto de elementos que forman parte del sistema en que se tienen que desplegar las diferentes operaciones de tratamiento relacionadas con el proyecto.

Existen diversas metodologías para describir un proyecto y detallar sus características, cada una con sus complejidades. Aquí intentaremos simplificarlo al máximo, teniendo en cuenta que esta guía quiere hacer una propuesta muy pragmática para la mayoría de las situaciones de evaluación. Aun así, en algún caso puede ser necesario recurrir a modelos de descripción de proyectos más completos y complejos.

El resultado de esta etapa es un documento que tiene que describir el proyecto y todas sus circunstancias; cuanto más detallada es la descripción, más sencillo es ejecutar la evaluación de impacto, ya que el propósito final no es otro que decidir de qué manera se afrontaran los potenciales riesgos, y para hacerlo es imprescindible conocer en

detalle las operaciones de tratamiento[31]. Este documento se divide en dos tipos de contenidos:

a) Una descripción funcional del proyecto o iniciativa que se está evaluando.

b) El detalle de los elementos más relevantes del sistema en el cual se tratarán los datos de carácter personal.

Aquí proponemos hacer la descripción funcional teniendo en cuenta el ciclo de vida de la información. De esta manera, nos aseguramos que recogemos todo lo que es relevante para la evaluación de impacto.

Hay diferentes modelos de representación del ciclo de vida de la información. El que utilizaremos aquí es simplificado, y ha sido específicamente pensado para los procesos de evaluación de impacto sobre la protección de datos[32].

Descripción funcional del tratamiento o proyecto según el ciclo de vida de los datos

Para describir el tratamiento o proyecto que implica el uso de datos personales, tenemos que considerar que el ciclo de vida de esta información se divide en cuatro[33] etapas:

Etapa 1. Entrada (de datos). El conjunto de la información utilizada por el sistema tiene un origen, u orígenes, que tiene que estar perfectamente identificado (un formulario en papel, un formulario web, una recogida automática o telefónica, unos datos calculados, una extracción de información, etc.). A la vez, cada origen está vinculado a uno o más proveedores de los datos (la misma persona interesada, terceros, un dispositivo, una base de datos preexistente, etc.). En definitiva, debemos conocer y describir con la máxima precisión como nos llegan los datos y quien los proporciona.

[31] Incorporado en la versión 2.0 de esta guía
[32] En el anexo D de la ISO/IEC 29134 se identifican como etapas del ciclo de vida de los tratamientos de datos personales: “collect”, “store”, “use”, “transfer” y “delete”
[33] Incorporado en la versión 2.0 de esta guía. Se ha simplificado el ciclo de vida de los datos respecto del que se utilizó en la primera versión de la guía

Aquí se debe tener en cuenta cuál es la base que legitima el tratamiento, por ejemplo si se basa en el consentimiento, en una obligación legal, en el interés legítimo, etc. En el caso del interés legítimo, como veremos, se debe argumentar la ponderación que se ha hecho entre el interés del responsable del tratamiento y la protección de los derechos y las libertades fundamentales de las personas.

En esta etapa también se incluyen las actividades de clasificación de los datos. Los datos que entran al sistema se tienen que clasificar de alguna manera, para identificar su utilidad para el tratamiento.

Algunos datos son útiles exclusivamente para identificar a las personas; otros permiten conocer aspectos de su personalidad, evaluar a la persona o conocer aspectos de su historia y circunstancias (estudios, familia, vida laboral, salud, etc.).

Y también describiremos las operaciones materiales de incorporación de la información en los sistemas de información, es decir, de qué manera se da de alta la información en el sistema, cuando se incorpora por primera vez. Esto incluye tanto a los mecanismos utilizados (aplicaciones y tecnologías) como a las personas o áreas implicadas en la introducción de la información del sistema.

En esta etapa de entrada de datos es relevante tener en cuenta los protocolos para verificar la autenticidad e integridad de los datos que se incorporan al tratamiento.

Etapa 2. Almacenamiento. Se trata de las operaciones y tecnologías que permiten conservar la información para recuperarla posteriormente (utilizarla). Por lo tanto, estarán definidas por determinadas tecnologías, ya sean bases de datos estructuradas, bases de datos documentales, simples sistemas de ficheros, etc.

Aquí se debe concretar la ubicación de la información, es decir, si se trata de un almacenamiento en la nube o en sistemas propios. También donde están situados geográficamente, cosa que también incluye los posibles sistemas alternativos y de apoyo (copias de seguridad y recuperación de sistemas).

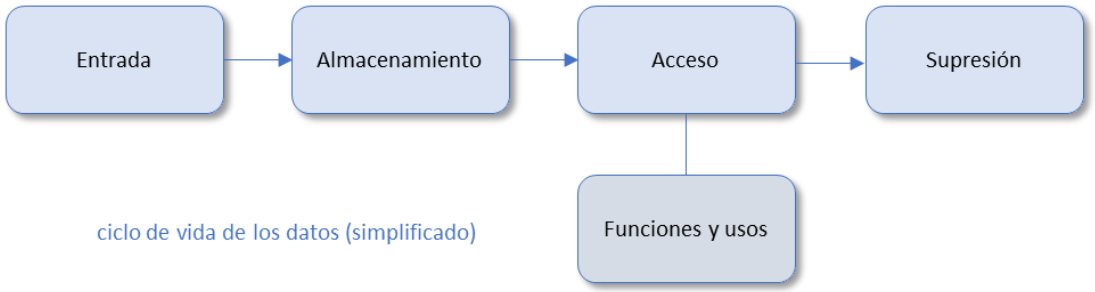
Etapa 3. Acceso. La etapa de acceso tiene que ver con las funciones o permisos de los diferentes usuarios del sistema, que se resumen en la posibilidad de consultar y modificar datos (información). Estas funciones facilitan los diferentes usos que se han previsto de la información: visualizar (por pantalla), imprimir, listar, agrupar, filtrar,

exportar, cruzar, analizar, calcular, actualizar, transformar, anonimizar, seudonimizar, etc.

En esta etapa se incluyen también las comunicaciones de datos hacia entornos ajenos o que no están bajo el control directo del responsable del tratamiento (salidas de información) [34].

Etapa 4. Supresión. La conservación de la información durante los plazos que esta resulte necesaria para atender a los fines vinculados a su obtención o tratamiento, es una cuestión que ha cogido una mayor relevancia con el RGPD.

En esta etapa hay que concretar durante cuánto tiempo se prevé conservar la información, motivando las razones de concreción de los plazos de conservación[35] y hay que describir los procedimientos de supresión, bloqueo y de destrucción definitiva de los datos.



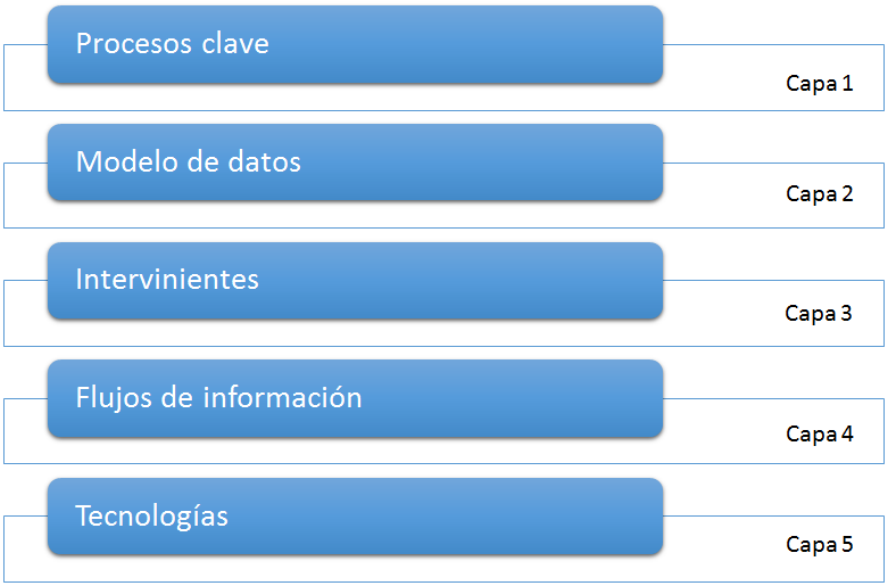
ciclo de vida de los datos (simplificado)

Este contenido tiene que formar parte del documento que elaboraremos para describir sistemáticamente las operaciones de tratamiento; en la parte 3 de esta guía se aporta, a título orientativo, una estructura y un índice de contenidos de este documento (véase modelo 4).

[34] Incorporado en la versión 2.0 de esta guía
[35] Incorporado en la versión 2.0 de esta guía

Detalle de los elementos más relevantes del sistema con un modelo de capas

El otro tipo de contenido de la descripción sistemática del tratamiento es una descripción del sistema por capas, concretamente se divide en cinco capas:



Capa 1. Procesos clave

Tenemos que identificar y describir los procesos clave del sistema que tenemos que evaluar. Consideraremos como proceso clave el conjunto de operaciones de tratamiento imprescindibles para que el sistema pueda alcanzar la finalidad para la cual se han definido; en general serán pocos procesos, puesto que habrá otros que serán complementarios o de soporte a los principales.

Aquí conviene identificar exclusivamente los que son realmente relevantes para el tratamiento de los datos de carácter personal. Esto quiere decir que no tenemos que considerar relevante, por ejemplo, un procedimiento de control como el de las copias de seguridad, que es relevante para la seguridad de los datos pero que no lo es en relación al uso funcional que se pretende dar a los datos.

Para identificar y describir los procesos relevantes, consideramos que un proceso está formado por un conjunto de operaciones de tratamiento de los datos personales (procedimientos), interrelacionadas entre sí, que se aplican a un conjunto de datos

(entrada del proceso) y que generan algún tipo de valor añadido, transformación de la información o resultado (salida del proceso).

Por ejemplo, tenemos que considerar como proceso clave de un tratamiento al conjunto de operaciones destinadas a recoger los datos de carácter personal; también lo será la comunicación de datos a terceros o un proceso de disociación de los datos. A pesar de que cada uno de estos procesos forme parte de un mismo tratamiento, cada uno tendrá unas características propias.

La propuesta que se hace en esta guía debe servir tanto para los tratamientos complejos como para los más simples. Por eso, incluso el conjunto del tratamiento se puede considerar como un único proceso, siempre y cuando sean tratamientos muy simples.

Para sistematizar y analizar la información sobre cada proceso clave, a título orientativo podemos utilizar la siguiente tabla:

Identificación del proceso	[nombre del proceso]			Código [si resulta útil]
Entrada(*) (clases de datos)	[A]	[B]		
	Mecanismo de recogida	Origen datos	Almacenamiento datos	Función principal
Operaciones de tratamiento	[por ejemplo: formulario web]	[por ejemplo: persona interesada]	[por ejemplo: base de datos en proveedor externo (nube)]	[por ejemplo: recogida de datos básicos de identificación para darse de alta en el servicio]
Resultado principal del proceso	[por ejemplo: incorporación de los datos básicos en el sistema, creación y entrega del mecanismo de acreditación y verificación de los medios de contacto (correo electrónico, teléfono, etc.)]			

(*) Recordatorio (de la plantilla de recogida de información sobre los datos y operaciones de tratamiento)

Clase A. Datos de carácter personal facilitados directamente por las personas afectadas

Clase B. Datos de carácter personal facilitados por terceros

Clase C. Datos de carácter personal ya disponibles anteriormente

Clase D. Datos de carácter personal capturados

Clase I. Datos de carácter personal calculados

Clase Z. Datos que inicialmente no se consideran de carácter personal

Capa 2. Modelo de datos

En esta segunda capa, identificaremos los datos de carácter personal relacionados con cada uno de los procesos que forman parte de la capa 1. Por lo tanto, se trata de disponer de una segunda capa de información y vincular las dependencias o relaciones entre procesos y conjuntos de datos.

Por eso, elaboraremos la lista de datos involucrados e indicaremos algunos atributos relevantes de cada dato, para la posterior evaluación de impacto:

- Si se trata de una categoría especial de dato.
- Si potencialmente podemos prescindir de este dato (aquí se hace una primera aproximación, sin determinar si efectivamente tiene que ser así).

Para recoger esta información, a título orientativo podemos utilizar una tabla como la siguiente:

Identificación proceso	[nombre del proceso]	Código [si se utiliza]	
		Crítico [valoración]*	
Datos	Descripción	Especial	Prescindible
[Identificador]	[Código único de identificación de la persona en el sistema]	☐	☐
[Nombre]	[Nombre]	☐	☐
[Apellidos]	[Apellidos]	☐	☐
[Usuario]	[Código usuario]	☐	☐
[Contraseña]	[Contraseña elegida por el usuario]	☐	☐
[Correo electrónico]	[Dirección de correo electrónico]	☐	☐
[Dirección IP]	[Dirección IP desde la cual se ha hecho el alta]	☐	☐
etc.	…	☐	☐

(*) Crítico: este nivel de criticidad es una primera valoración, a título de aviso, con la cual consideramos que para el tipo de datos que trata este proceso tiene un potencial de riesgo relevante o significativo. En la evaluación de los riesgos lo valoraremos de una manera más fundamentada y, si procede, revisaremos esta primera valoración; de hecho, la EIPD se considera un proceso iterativo, ya que a medida que avanzamos en la evaluación y vamos concretando aspectos relevantes del tratamiento, se producirá una cierta retroalimentación que obligará a modificar o revisar aspectos ya analizados. Para marcar la criticidad podemos utilizar la escala tradicional de bajo, medio y alto, pero se pueden utilizar otras.

Hay que recordar que mucha de esta información se puede haber recogido en la etapa previa a la evaluación (cuando se ha analizado la necesidad de hacer la EIPD). En todo caso, se debe asegurar que no hay datos que se prevé utilizar y que no se detectaron o utilizaron en la mencionada etapa previa.

Capa 3. Intervinientes

Por intervinientes[36] en el tratamiento entendemos todas las personas físicas o jurídicas que, de manera individual o colectiva, están implicadas en el tratamiento de los datos de carácter personal, entendida esta implicación en un sentido amplio.

Por lo tanto, son partes intervinientes las personas afectadas por las operaciones del tratamiento, los empleados del responsable del tratamiento, el mismo responsable del tratamiento, los encargados de tratamiento, las empresas proveedoras de soluciones TIC o de cualquiera otro servicio que involucre a los datos personales, terceros a los cuales se los comuniquen los datos, etc.

Cada uno de estos intervinientes tiene que estar adecuadamente identificado y tiene que tener asignado un rol en relación a las operaciones de tratamiento previstas o en un proceso concreto (conjunto de operaciones de tratamiento de datos personales), cosa que implica unas funciones y responsabilidades en relación al tratamiento de los datos de carácter personal.

Como en las capas anteriores, puede ser útil elaborar una sencilla ficha con las informaciones básicas de cada interviniente.

	Procesos			
Intervinientes	[código proceso]	[código proceso]	[código proceso]	etc.
[...]	x	x	x	□
	Función o rol principal: [...]			
[...]	x	□	□	□
	Función o rol principal: [...]			

[36] A la ISO/IEC 29134 se identifican como “stakeholders”

La ISO / IEC 29134 clasifica la parte intervinientes en cuatro grupos: personas afectadas, responsable del tratamiento, encargado del tratamiento y terceras partes; esta clasificación se puede utilizar para concretar la función o rol principal[37].

Capa 4. Flujos de información

Los datos personales objeto de tratamiento siguen un determinado recorrido entre los diferentes intervinientes, de acuerdo con las operaciones de tratamiento previstas. Se debe describir estos movimientos de información, de forma que dispongamos de un mapa claro de quien tiene acceso a datos personales concretos, y en qué momento.

Para hacerlo, será útil tener en cuenta lo que ya se ha tratado en relación al ciclo de vida de la información.

Para recoger y sistematizar la información de esta capa de flujos de información, podemos utilizar una tabla como la que se propone a continuación.

Proceso	[alta usuario]		Código		[código]
Operaciones (*)	**Entrada**	**Almacenamiento**	**Acceso**	**Supresión[38]**	
Intervinientes origen					Intervinientes destino
[usuario]	x	□	□	□	[proveedor alojamiento aplicación] [responsable del tratamiento]
[proveedor alojamiento aplicación]	x	x	□	□	[responsable del tratamiento]
[responsable del tratamiento]	x	x	x	x	n/a
etc.	□	□	□	□	etc.

[37] Incorporado en la versión 2.0 de esta guía
[38] Incorporado en la versión 2.0 de esta guía

(*) Señalaremos las operaciones en las cuales interviene cada cual, de acuerdo con la fase de ciclo de vida de los datos en que se ubican las operaciones.

Capa 5. Tecnologías

En esta última capa, identificaremos las tecnologías más relevantes para el tratamiento de los datos de carácter personal. No se trata de un análisis técnico de las diferentes aplicaciones, infraestructuras de red, sistemas de almacenamiento, etc. del conjunto del tratamiento que estamos describiendo y, por lo tanto, el grado de detalle no ha ser técnico, sino exclusivamente conceptual.

Por eso, basta de identificar que hay, por ejemplo:

- Un entorno de servidores virtuales de un proveedor externo, en el cual se sitúan todas las infraestructuras relacionadas con el tratamiento (en algún caso, puede ser relevante introducir algún dato de carácter técnico).
- Una aplicación determinada (podemos identificar, o no, el producto concreto; esto depende de si puede ser relevante).
- Una aplicación para dispositivos móviles (app).
- El uso de dispositivos biométricos.
- Una base de datos (puede ser relevante conocer qué base de datos se utilizará, y en qué versión).
- Dispositivos que se utilizan en el contexto de las operaciones de tratamiento: ordenadores personales, portátiles, teléfonos inteligentes, tabletas, etc.

Cómo que estamos describiendo aspectos funcionales del proyecto, todavía no se deben identificar los elementos de seguridad, como los cortafuegos, sistemas de detección de intrusos y de prevención de fuga de información, sistemas de copias seguridad, soluciones de control de acceso, etc. En general, estos elementos forman parte de las decisiones relacionadas con la mitigación de los riesgos y, por consiguiente, no están vinculados estrictamente a las funcionalidades del proyecto.

No obstante, y a pesar de que no es el objetivo que pretendemos lograr con la descripción de las operaciones de tratamiento, como que se trata de un método abierto, esta información de elementos de seguridad ya se puede incorporar en esta primera aproximación tecnológica al sistema.

Desde el punto de vista de la recogida y sistematización de la información de esta capa, basta hacer un inventario de las tecnologías que intervienen y la vinculación que tienen con los procesos.

Una manera de organizar la información es, primero, identificar el hardware e infraestructuras técnicas, para después ir añadiendo el software que sea relevante desde la perspectiva del tratamiento de los datos de carácter personal.

En cualquier caso, hay herramientas o productos orientados a elaborar los inventarios de activos de sistemas de información, que pueden ser perfectamente válidos para ayudarnos a identificar y clasificar la información relacionada con las tecnologías utilizadas en el tratamiento de datos de carácter personal que estamos evaluando.

Si alguna operación implica el tratamiento no automatizado de los datos, por ejemplo un archivo de documentos en papel, lo tenemos que identificar como una técnica de tratamiento que se aplica a las operaciones con los datos y lo podemos inventariar como un activo más.

Si añadimos la capa de tecnologías, ya tenemos completo el mapa del sistema en el cual se llevarán a cabo las operaciones de tratamiento que se tienen que evaluar.

Tal como prevé el RGPD, dispondremos de una descripción sistemática completa de las operaciones de tratamiento, que podemos incorporar a un documento con los contenidos propuestos en el modelo 4 de esta guía.

Representación gráfica de las operaciones de tratamiento

Además de incorporar la información de manera descriptiva y de añadir tablas, que facilitan el análisis posterior, también puede ser útil incorporar esquemas y representaciones gráficas de las operaciones de tratamiento y de los diferentes elementos que intervienen (diagrama o gráfico de cada una de las capas[39]). Aun así, en tratamientos complejos esta representación gráfica puede ser complicada y, por lo

[39] Incorporado en la versión 2.0 de esta guía

tanto, sólo es conveniente introducirla si sirve para aportar más claridad y comprensión del conjunto del tratamiento o de operaciones de tratamiento específicas.

Para completar la descripción del tratamiento, hace falta que añadamos otros contenidos, como podrían ser las finalidades del tratamiento y la evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento, que se tratan en el siguiente apartado de esta guía.

OBJETIVOS Y FINALIDADES DEL TRATAMIENTO

EVALUACIÓN DE LA NECESIDAD Y PROPORCIONALIDAD DE LAS OPERACIONES DE TRATAMIENTO

El documento que describe el tratamiento debe incluir algunos aspectos esenciales para cualquier tratamiento de datos de carácter personal, como es la base de legitimación, la finalidad o la necesidad y proporcionalidad de las operaciones de tratamiento que se prevé llevar a cabo.

El objetivo de la iniciativa que se debe evaluar (el proyecto) es el resultado que esperan obtener los promotores (responsables del tratamiento). Por lo tanto, no necesariamente es la finalidad específica del tratamiento, o de operaciones concretas de tratamiento, a pesar de que evidentemente los objetivos de la organización pueden formar parte de la finalidad del tratamiento. En el momento de ejecutar la EIPD conviene tener claros estos objetivos, como información adicional para contextualizar mejor qué se pretende llevar a cabo con el nuevo proyecto.

Los objetivos del proyecto pueden ser de índole muy diversa (económicos, de eficacia, de negocio, de mejora, etc.) y están estrechamente vinculados a la actividad del responsable del tratamiento, ya sea de cariz público o privado. Podemos considerar que los objetivos también están vinculados con los motivos para llevar a cabo un determinado tratamiento.

Por ejemplo, para limitar el acceso a una instalación deportiva municipal, se puede plantear un proyecto de control de acceso mediante un sistema biométrico (como por ejemplo reconocimiento facial), con objeto de evitar que accedan personas que no están abonadas a la instalación; este es el objetivo principal del promotor de la iniciativa. Para conseguir este objetivo, el promotor debe diseñar unas operaciones de tratamiento de datos de carácter personal, que implican una actividad de tratamiento que tiene una finalidad: el control de acceso a unas instalaciones.

El ejemplo planteado se concreta en la puesta en marcha de un mecanismo de control de acceso basado en reconocimiento facial, que implica hacer diversas operaciones de tratamiento de datos de carácter personal:

- Obtener una fotografía del rostro de cada persona y un patrón facial de reconocimiento.

- Vincular este patrón facial a la base de datos de usuarios (que puede incluir información sobre el estado de pago de las cuotas o de los servicios a los cuales puede acceder cada abonado, o del uso que hacen de las instalaciones).

- Capturar la imagen del rostro cada vez que se intenta acceder a la instalación y compararla con el patrón de que se dispone, para decidir si se permite el acceso a aquella persona.

Para determinar la necesidad y proporcionalidad de las operaciones de tratamiento[40] es necesario que tengamos clara la finalidad para la cual se ha diseñado cada operación de tratamiento concreta, junto con la finalidad del conjunto del tratamiento y los objetivos que se persiguen.

Describir la finalidad también forma parte del contenido mínimo de la evaluación de impacto (véase el modelo 4, de índice de contenidos del documento que debe describir el tratamiento).

La base de legitimación del tratamiento

El tratamiento lícito de datos personales implica, en primer lugar, que los datos se traten de acuerdo con el consentimiento de la persona titular de los datos (interesado), o bien en conformidad con «alguna otra base legítima establecida», ya sea el mismo RGPD o cualquier otra regulación de la Unión Europea o nacional de los estados miembros.

El artículo 6 del RGPD regula los supuestos en que se considera que el tratamiento de datos personales es lícito. Si la base de licitud del tratamiento es el consentimiento[41] del interesado, el responsable del tratamiento debe poder demostrar que ha obtenido este consentimiento para el tratamiento.

[40] Incorporado en la versión 2.0 de esta guía
[41] Ver WP 259. "Guidelines on Consent under Regulation 2016/679"

Los artículos 13 y 14 del RGPD[42] regulan la información que se debe proporcionar a las personas interesadas en relación a los tratamientos que se pretenden llevar a cabo y, en este sentido, la APDCAT publicó la *Guía para el cumplimiento del deber de informar en el RGPD*[43].

Cuando el artículo 35.7 del RGPD, en el apartado dedicado a la descripción sistemática de las operaciones de tratamiento y de las finalidades del tratamiento, establece los contenidos mínimos de la EIPD, también indica que si el interés legítimo es la base que legitima el tratamiento, se debe tener en cuenta este interés legítimo al describir el tratamiento objeto de evaluación.

El interés legítimo se puede utilizar como base de licitud de un tratamiento «siempre que no prevalezcan los intereses o los derechos y libertades de la persona interesada» y teniendo en cuenta las expectativas razonables de las personas afectadas por el tratamiento, basadas en la relación que tienen con el responsable del tratamiento. El uso del interés legítimo como base de licitud del tratamiento requiere una evaluación cuidadosa. Esta evaluación cuidadosa a la cual se refiere el RGPD implica que, cuando la licitud del tratamiento se basa en el interés legítimo del responsable del tratamiento (o de un tercero), se deben sopesar estos intereses y los de las personas que se verán afectadas.

Nos remitimos al Dictamen del GT29 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento, en virtud del artículo 7 de la Directiva 95/46/CE (WP217)[44], especialmente el anexo 1, que incorpora una «Guía rápida sobre cómo llevar a cabo la prueba de sopesamiento del artículo 7, letra f)». A pesar de que esta guía se refiere al interés legítimo recogido en la Directiva, con las adecuaciones pertinentes, también es útil en el contexto del RGPD.

El artículo 35.7.*a se* refiere expresamente a la descripción del interés legítimo del responsable del tratamiento, que se tiene que incluir si se utiliza como base de licitud del tratamiento.

[42] Veure WP 260. "Guidelines on Transparency under Regulation 2016/679"
[43] http://apdcat.gencat.cat/ca/documentacio/rgpd/altres_documents_dinteres/
[44] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_es.pdf

Necesidad y proporcionalidad del tratamiento

Cabe señalar que no es objeto de esta guía orientar sobre cómo hacer la valoración de la necesidad y proporcionalidad de las operaciones de tratamiento, pero la letra *b* del artículo 35.7 del RGPD establece que es necesario que «una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento en cuanto a su finalidad» forme parte del contenido mínimo de la EIPD. Esta cuestión la debemos vincular con lo que recoge el considerando 39 del RGPD: «Los datos personales sólo se deben tratar si la finalidad del tratamiento no se puede hacer razonablemente por otros medios».

El RGPD no concreta cómo se tiene que hacer esta evaluación de la necesidad y proporcionalidad de los tratamientos. Para concretarla, el WP211 del GT29 nos puede resultar parcialmente útil, es el Dictamen 01/2014 sobre la aplicación de los conceptos de necesidad y proporcionalidad y la protección de datos en el sector de los organismos con funciones coercitivas. A pesar de que el dictamen está centrado en un contexto muy concreto, algunos de los aspectos generales que recoge sobre estos principios nos pueden ser de utilidad.

En cuanto a determinar la necesidad de llevar a cabo un tratamiento, el concepto no se tiene que interpretar de una manera demasiado amplia, ya que esto puede llevarnos a la conclusión de que el tratamiento es necesario en todos los casos, puesto que da respuesta o está vinculado a un objetivo relacionado con la actividad del responsable del tratamiento; tampoco se tiene que abordar con exceso de literalidad, ya que complicaría la justificación del tratamiento.

> Se debe determinar si se cumple el requisito de necesidad, tanto en relación a la actividad del responsable del tratamiento como en relación a la finalidad del mismo tratamiento.

Respecto de la finalidad del tratamiento, se deben recordar los elementos esenciales, es decir: las finalidades tienen que estar definidas de manera determinada, explícita y legítima. Así mismo, debemos tener en cuenta lo que recoge el considerando 39 del RGPD: «Cualquier tratamiento de datos personales tiene que ser lícito y leal»; por lo tanto, el punto de partida es que la finalidad se ajuste a estos requisitos.

El considerando 39, que ya se ha mencionado, establece que los datos personales tienen que ser adecuados, pertinentes y limitados a lo necesario para los fines para los

cuales se tratan. Además, se debe garantizar «que el plazo de conservación se limite a un mínimo estricto».

Respecto de la necesidad del tratamiento, también tenemos que considerar que los datos personales sólo se tienen que tratar si la finalidad no se puede lograr "razonablemente" por otros medios, es decir, sin tratar datos personales

Proporcionalidad de las operaciones de tratamiento.

La sentencia del Tribunal Constitucional 207/1996 establece que la proporcionalidad es una exigencia común y constante para que cualquier medida restrictiva de derechos fundamentales sea constitucional.

Las autoridades de protección de datos a menudo señalan que para comprobar si una operación de tratamiento supone una medida restrictiva de un derecho fundamental, esta operación tiene que superar los tres puntos del llamado juicio de proporcionalidad:

- Si la medida puede conseguir el objetivo propuesto (juicio de idoneidad).
- Si, además, es necesaria, en el sentido de que no existe otra más moderada para conseguir este propósito con la misma eficacia (juicio de necesidad).
- Si la medida es ponderada o equilibrada, porque se derivan más beneficios o ventajas para el interés general que no perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

Por lo tanto, la proporcionalidad tiene que ver con evaluar si la finalidad que se persigue se puede conseguir por otros medios, por ejemplo: usando otros datos (menos datos), reduciendo el universo de personas afectadas (cuantitativamente o cualitativamente hablando), usando otras tecnologías menos invasivas o aplicando otros procedimientos o medios de tratamiento (modificando los inicialmente previstos), etc.

La proporcionalidad se ha tratado especialmente en el ámbito de la videovigilancia, por lo que nos puede ser útil tener en cuenta como se aborda esta cuestión en las instrucciones de videovigilancia de las autoridades de control.

Así, la Instrucción 1/2009, de 10 de febrero, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia de la APDCAT[45], hace referencia a los tres análisis que se deben hacer para valorar el juicio de proporcionalidad al que ya hemos aludido:

> «(…) una medida intrusiva como la que estamos analizando sólo se puede considerar constitucionalmente legítima si resulta proporcionada a través de un triple análisis de la necesidad de la medida, su idoneidad y su carácter proporcional en sentido estricto. Es decir, cuando no se pueda alcanzar la misma finalidad mediante medidas menos intrusivas o que comporten menos riesgos para las personas»

El artículo 7.2 de la instrucción mencionada describe el proceso de ponderación que se tiene que hacer respecto de los diferentes derechos y bienes jurídicos que pueden entrar en conflicto, de forma que obliga a analizar, en relación a los sistemas de videovigilancia:

> «Con carácter previo a la instalación, las personas responsables de la utilización de sistemas de videovigilancia deben ponderar los diferentes derechos y bienes jurídicos en juego, analizando:
>
> a) La necesidad de utilizar estos sistemas.
>
> b) La idoneidad de la instalación de sistemas de videovigilancia para alcanzar la finalidad perseguida.
>
> c) El riesgo que puede suponer para los derechos de las personas, teniendo en cuenta las características del sistema de videovigilancia, las circunstancias de la captación y las personas afectadas.
>
> d) La ausencia de medidas de vigilancia alternativas que comporten un riesgo menor»

En el momento de evaluar hasta qué punto las operaciones de tratamiento previstas son necesarias y proporcionadas, se deben tener en cuenta algunos de los principios relativos al tratamiento que recoge el artículo 5.1 del RGPD:

> a) Principio de limitación de la finalidad: los datos recogidos no se pueden utilizar de manera incompatible con la finalidad para la cual se recogieron.
>
> b) Principio de minimización de datos: los datos que se ha previsto tratar deben ser adecuados, pertinentes y limitados a lo que es necesario en relación con las finalidades (no excesivos).

[45] http://apdcat.gencat.cat/ca/autoritat/normativa/disposicions/instruccions/

c) Principio de limitación del plazo de conservación: los datos no se tienen que mantener más tiempo del necesario para las finalidades del tratamiento.

En definitiva, en relación con la EIPD, debemos responder de manera argumentada dos preguntas:

- ¿El tratamiento, tal como se ha definido, es necesario para la finalidad prevista?
- ¿Las operaciones de tratamiento resultan proporcionadas a las finalidades perseguidas?

Respecto de la adhesión a códigos de conducta

Para finalizar con los aspectos descriptivos del tratamiento, hacemos una breve referencia al hecho que, al describir el tratamiento, debemos tener en cuenta y reflejar si el responsable del tratamiento está adherido a algún código de conducta (los códigos de conducta se regulan en el art. 40 y siguientes del RGPD).

También identificaremos y describiremos si de esa adhesión se deriva alguna cuestión que se deba tener en cuenta en el momento de realizar la EIPD, más allá de lo que dispone la propia regulación, como por ejemplo, que esa adhesión implique aplicar una determinada guía de evaluación, o que el mismo código de conducta establezca en qué casos se debe hacer la EIPD, o haya previsiones concretas sobre el ejercicio de derechos, medidas de seguridad, gestión de riesgos, etc., que se deben considerar en el momento de hacer la EIPD.

GESTIÓN DE RIESGOS: ASPECTOS GENERALES

Hemos llegado a la parte central de la EIPD. Las etapas anteriores (valorar la necesidad de evaluación y descripción del tratamiento) nos han servido para recoger la información que nos tiene que servir para empezar a evaluar cómo las operaciones de tratamiento pueden afectar a los datos de carácter personal, y en consecuencia a las personas y sus derechos y libertades.

Si hemos hecho la descripción de los tratamientos adecuadamente, tenemos casi toda la información necesaria para empezar a evaluar el impacto. Por lo tanto, la precisión y la eficacia del proceso de evaluación, depende en gran medida, de que estas actividades previas se ejecuten correctamente.

El artículo 35.7 del RGPD también prevé el siguiente contenido mínimo de las EIPD:

- Una evaluación de los riesgos para los derechos y las libertades de los interesados.
- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos para garantizar la protección de datos personales y para demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

En esta etapa, identificaremos los potenciales escenarios de riesgo (PER) que pueden afectar negativamente a las personas, debido al tratamiento de sus datos: acontecimientos no deseados en el tratamiento de los datos de carácter personal.

Este impacto se concreta en dos tipos de consecuencias:

- Un resultado de daño o perjuicio material o inmaterial que afecta a las personas (discriminación, rechazo, daño económico, perjuicio laboral, intromisión en la intimidad, etc.).
- Una vulneración de cualquier derecho o libertad fundamental de las personas, particularmente el derecho a la protección de los datos de carácter personal.

La gestión de los riesgos relacionados con las operaciones de tratamiento sujetas al RGPD implica que todas las decisiones relacionadas con el tratamiento de los datos de carácter personal, y no sólo las vinculadas a la seguridad de los tratamientos, se deben sustentar en la gestión de los riesgos.

En consecuencia, el RGPD incorpora la gestión de riesgos como una actividad que el responsable del tratamiento[46] debe llevar a cabo para seleccionar y adoptar las medidas de carácter técnico y organizativo más adecuadas para:

- Garantizar que el tratamiento se hace según lo que prevé el RGPD.
- Demostrar que el tratamiento es conforme al RGPD (responsabilidad proactiva).

Cuando el RGPD establece que se deben evaluar los riesgos inherentes a los tratamientos, los concreta en el riesgo a que se vulneren los derechos y las libertades de las personas, como consecuencia del tratamiento de sus datos personales.

La gestión de riesgos que prevé el RGPD va más allá de evaluar la exposición al riesgo de los sistemas de información o de los datos, o de los riesgos para la organización.

El RGPD identifica como situaciones de riesgo para los derechos y las libertades las siguientes:

- Se priva a los interesados de sus derechos y libertades, que incluye cuando se impide su ejercicio normal y libre.
- Se provocan daños y perjuicios físicos, materiales o inmateriales a las personas interesadas.
- Se revelan categorías especiales de datos personales, o relativas a condenas e infracciones penales, durante el tratamiento.
- Se crean o se utilizan perfiles personales.
- Se tratan los datos personales de colectivos especialmente vulnerables, incluidos los niños.
- Se trata una gran cantidad de datos personales o datos que afectan a un gran número de personas.

Los riesgos pueden ser variables, tanto en lo referente a la probabilidad como a la gravedad. Por eso, en el momento de seleccionar y aplicar las medidas técnicas y organizativas se debe tener en cuenta:

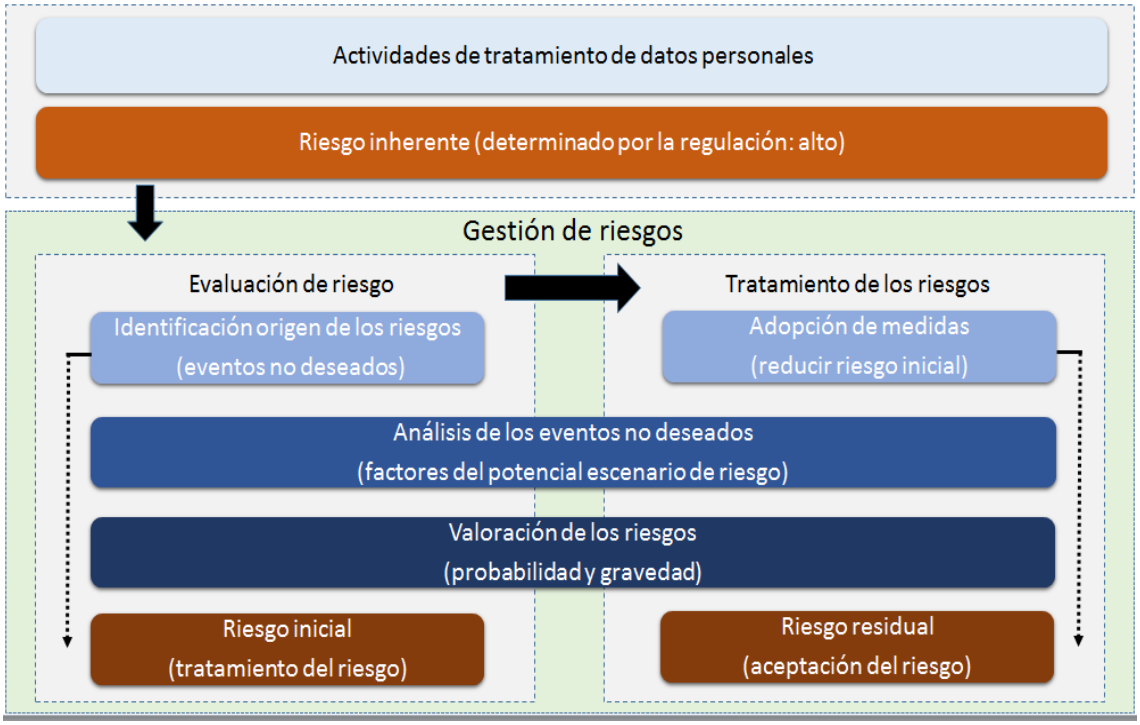
- La probabilidad de que se produzca la situación que pone en riesgo derechos y libertades como consecuencia del tratamiento de datos personales.

[46] Y también a los encargados de tratamientos

– La gravedad de las consecuencias, si sucede la situación que pone en riesgo derechos y libertades

En consecuencia, hay que hacer una estimación, de la manera más objetiva posible, del nivel o de la zona de riesgo, en que se sitúan las operaciones de tratamiento o el tratamiento en su conjunto. La evaluación o estimación de los riesgos debe permitir identificar si el tratamiento supone un alto riesgo.

En esta guía, abordaremos cada una de las etapas de la gestión de riesgos en el contexto de una EIPD, que se recogen en el esquema siguiente:



El punto de partida es que cualquier tratamiento de datos de carácter personal implica potencialmente algún tipo de riesgo. Esto significa que la recogida de información relativa a personas físicas para tratarla con técnicas diversas comporta que esta información quede expuesta a riesgos de índole diversa.

Siempre hay un riesgo inherente al tratamiento, por el hecho de llevarlo a cabo. Lo que persigue el proceso de gestión de riesgos es mantenerlo en unos niveles aceptables.

El legislador ya ha considerado que hay actividades de tratamiento que presentan, de manera inherente, un riesgo alto. Por eso, en un primer momento el responsable del tratamiento se debe limitar a verificar si las actividades de tratamiento que pretende hacer encajan en los supuestos en que el RGPD prevé este nivel significativo de riesgo, y actuar en consecuencia.

Ya hemos visto que se debe analizar si un tratamiento, de acuerdo con sus características, tiene que ser objeto de una evaluación de impacto. Gestionar los riesgos implica evaluarlos (art. 35.7.*c* del RGPD) y tratarlos (art. 35.7.*d* del RGPD). Para evaluar el riesgo, se deben llevar a cabo tres tipos de actividades:

1. Las que tienen por objeto identificar el origen de los riesgos, es decir, reflexionar sobre los potenciales escenarios de riesgo a los cuales pueden estar expuestos los datos personales.

2. El análisis de las situaciones que generan riesgo, teniendo en cuenta los diversos factores y características que pueden entrar en juego en el momento de hacer una estimación del nivel de riesgo que implican.

3. La valoración de los riesgos, teniendo en cuenta la probabilidad de que un acontecimiento no deseado se produzca y la gravedad que puede tener (consecuencias potenciales).

El resultado de la primera evaluación de riesgos nos indica el nivel de riesgo inicial, que debe ser objeto de reducción, para procurar aumentar la capacidad de control que podemos ejercer sobre el riesgo que generan las operaciones de tratamiento. Este tratamiento de los riesgos se debe encaminar a seleccionar medidas de carácter técnico y organizativo para reducir la probabilidad y gravedad de las operaciones de tratamiento.

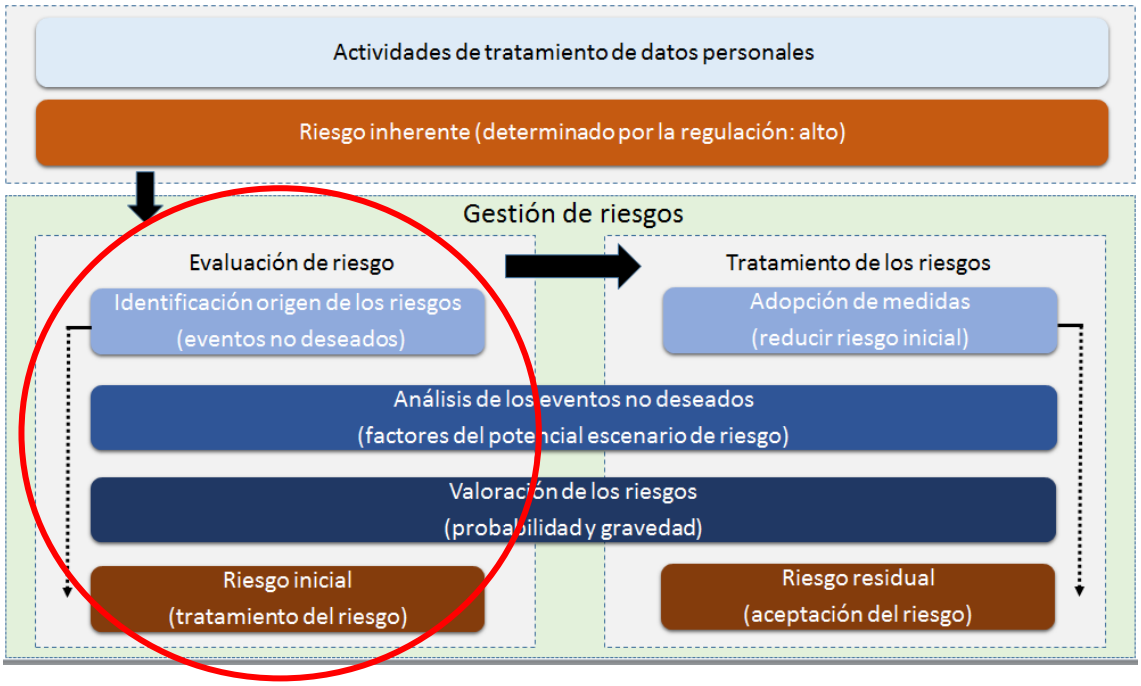
Estas nuevas medidas tienen que reducir el nivel de riesgo de las operaciones de tratamiento. Para verificarlo, debemos volver a analizar y valorar los riesgos, teniendo en cuenta las nuevas medidas previstas. De este segundo proceso de análisis y valoración resulta un riesgo residual, es decir, un riesgo que, a priori, ya no podemos reducir más; por lo tanto, lo debemos reconocer y aceptar.

EVALUACIÓN DE LOS RIESGOS Y MEDIDAS PARA AFRONTARLOS

La gestión de riesgos es la actividad que requiere más atención y que probablemente implica más dificultad de ejecución. El nivel de exhaustividad que queramos dar a la evaluación y al tratamiento de los riesgos depende, en gran medida, de las características del tratamiento. La propuesta que se hace aquí intenta conjugar facilidad y utilidad, sin perder eficacia, a pesar de que también se pueden utilizar otros métodos de gestión de riesgos, adaptándolos a la protección de datos; por lo tanto, si ya se utilizan otras metodologías de gestión de riesgos, conviene valorar si se adaptan a las EIPD[47].

A pesar de que se intentan introducir elementos objetivos de valoración, algunos de los factores de la evaluación de riesgos tienen siempre un componente subjetivo. En este sentido, el conocimiento y la experiencia del profesional que identifica, analiza y valora los riesgos es clave para que el diagnóstico sea lo más preciso posible. Por eso, el conocimiento y la experiencia se deben aplicar siempre como mecanismo de corrección de las valoraciones de riesgos que se consideren desviadas o no alineadas con la realidad de cada escenario de riesgo analizado.

Centrémonos ahora en las actividades de gestión de riesgos vinculadas a la evaluación de riesgos, es decir: la identificación, el análisis y la valoración.



[47] Por ejemplo, en el proyecto de LOPD se prevé que el Esquema Nacional de Seguridad adapte los criterios de determinación del riesgo a lo que prevé el RGPD (Disposición adicional primera)

Etapas de la evaluación de riesgos: identificación, análisis y valoración de riesgos

Trataremos los riesgos desde la perspectiva de cada proceso clave que hemos identificado. En tratamientos sencillos puede ser más eficaz valorar el conjunto de procesos clave como uno sólo y considerar el tratamiento como un único proceso.

Como punto de partida, haremos la valoración de los procesos clave que ya tenemos identificados y de los cuales tenemos información de los datos, operaciones, intervinientes, flujos de información y tecnología.

Si detectamos algún proceso secundario que no hemos considerado clave y que puede aportar algún elemento relevante en relación al riesgo a que se exponen los datos personales, lo podemos incorporar al proceso de evaluación de riesgos en cualquier momento, recordemos que la evaluación de impacto es un proceso iterativo[48].

Del mismo modo, si consideramos que hay un proceso clave concreto que, por su entidad, relevancia, impacto potencial, etc., se debe analizar de manera más detallada, podemos identificar, analizar y valorar los riesgos del conjunto del tratamiento a partir de este proceso de manera individualizada. Esto puede surgir en actividades de tratamiento que tengan algún proceso de mucho peso en el conjunto del tratamiento.

Otra cuestión a tener en cuenta es que las actividades que desarrollaremos no pretenden sustituir la gestión de riesgos tradicional de los sistemas de información (medidas de seguridad de la información), de forma que muy probablemente en sistemas complejos esos riesgos para la seguridad de los datos se deberán de analizar de manera particular.

El método de evaluación de los riesgos debe ser sistemático. Por eso, la fase de evaluación de riesgos se estructura en tres etapas:

- Identificación de los riesgos
- Análisis de los riesgos
- Valoración de los riesgos

[48] Incorporado en la versión 2.0 de esta guía

1. Identificación del riesgo

En primer lugar, debemos identificar los potenciales escenarios de riesgos que implican un daño o perjuicio para las personas afectadas por el tratamiento de los datos, ya sea porque suponen un daño o perjuicio material directo, porque vulneran principios o derechos y libertades o porque el responsable del tratamiento incumple alguna obligación.

Cómo ya hemos avanzado, como regla general debemos evaluar el tratamiento a partir de cada proceso clave, teniendo en cuenta el alcance de la posible vulneración de principios y derechos relacionados con el derecho a la protección de los datos de carácter personal, el incumplimiento de obligaciones o la afectación en otros derechos y libertades.

Se puede hacer una evaluación de riesgos del conjunto del tratamiento. Si se hace así, debe prestarse atención a que se podría estimar un nivel aceptable de riesgo en su conjunto, pero que un proceso clave concreto genere un riesgo superior, que puede quedar oculto en el análisis conjunto.

A pesar de que el planteamiento es flexible, obliga a reflexionar previamente sobre cuál es la orientación más óptima para la gestión de riesgos, que es una cuestión muy vinculada a las características de cada tratamiento.

En la parte 3 de la guía se adjunta una lista de potenciales escenarios de riesgo genéricos (en el modelo 5 se han recogido un total de setenta[49]), que pueden servir de base para concretar los que aplicarían a un tratamiento concreto. Se trata de una lista de situaciones de riesgo genéricas que pueden aparecer en las diferentes operaciones de tratamiento que se tienen que evaluar, que se han estructurado de acuerdo con el contexto que afectan: principios, derechos, obligaciones, otros derechos y libertades, y daños y perjuicios directos; para facilitar su sistematización e identificación, se les ha asignado un código (que se puede modificar para adaptarlo a las circunstancias concretas de cada tratamiento).

Clasificar los PER permite hacer un análisis más detallado, puesto que facilita saber si los riesgos más significativos están fundamentalmente centrados, por ejemplo, en la vulneración de derechos o bien en el cumplimiento de obligaciones. La agrupación que se ha propuesto se puede modificar de acuerdo con la manera como se quieran

[49] Incorporado a la versión 2.0 de esta guía: se han añadido escenarios de riesgo relacionados con los daños y perjuicios directos que pueden causar las operaciones de tratamiento

visualizar los riesgos en el momento de trasladarlos a un mapa de riesgos del tratamiento, como veremos más adelante.

Las obligaciones relacionadas con la seguridad de la información se pueden segregar como una obligación especial y darle un tratamiento diferenciado; por eso, se han destacado en las listas de potenciales escenarios de riesgo. No se trata de una lista cerrada, es decir que se puede ampliar.

En cualquier caso, no debemos olvidar que estamos ante unos tratamientos que se están diseñando, por lo tanto, cuando las operaciones de tratamiento estén efectivamente implantadas, habrá que gestionar los riesgos para la seguridad de los datos desde la perspectiva de las medidas de seguridad efectivamente implantadas[50].

Una vez identificados todos los potenciales escenarios de riesgo del tratamiento que se está evaluando, pasamos a la etapa siguiente de la EIPD: el análisis de los riesgos.

[50] Incorporado en la versión 2.0 de esta guía

2. Análisis del riesgo

El objetivo del análisis de riesgos es determinar la probabilidad de que se produzcan situaciones no deseadas, así como su gravedad. Por lo tanto, concretaremos y describiremos qué medidas se han previsto para los procesos clave del tratamiento que estamos evaluando, que pueden tener como efecto:

- Reducir la probabilidad del PER.
- Reducir su gravedad, si se produce el PER

Debemos analizar las diferentes medidas que se han previsto inicialmente para reducir los riesgos del tratamiento (en sus dos dimensiones: probabilidad y gravedad). De esta forma, podemos valorar el nivel de riesgo inicial de las operaciones de tratamiento que se han diseñado.

Si no se toma ningún tipo de medida para mitigar la probabilidad y la gravedad de un potencial escenario de riesgo, es altamente probable que se produzca y, a priori, puede tener unas consecuencias muy graves (el nivel de riesgo se valora en la siguiente etapa de evaluación de los riesgos).

En esta etapa de análisis, especialmente debemos identificar las diferentes medidas que se ha pensado adoptar para reducir la probabilidad y la gravedad de cada PER del tratamiento, y cualquier otra circunstancia que pueda modificar el riesgo.

Podemos considerar que las medidas orientadas a reducir la probabilidad son de carácter preventivo, mientras que las medidas destinadas a reducir el impacto son de tipo reactivo o de recuperación, puesto que están encaminadas a intentar reducir la gravedad.

Un vez tenemos una lista de medidas previstas para cada PER, el paso siguiente es valorar en qué nivel de riesgo inicial se sitúan las operaciones de tratamiento.

3. Valoración del riesgo

Una vez identificadas todas las medidas previstas inicialmente, se debe valorar su probabilidad y su gravedad. Esto nos proporciona información del nivel de riesgo inicial de cada PER (y, si procede, de cada grupo de riesgos) y nos permite, por ejemplo, elaborar un primer mapa de riesgos del tratamiento que conecte la probabilidad y la gravedad.

Para hacerlo, podemos utilizar cualquier escala de valores que nos permita ubicar de la forma más precisa posible el nivel de riesgo en que se sitúa el tratamiento que estamos evaluando. Pueden ser valores entre el 1 y el 10, o entre el 1 y el 3 e incluso, podemos utilizar valores porcentuales. Aquí proponemos utilizar una escala entre el 1 y el 5.

Probabilidad	
Descripción	Nivel
Inminente	5
Muy probable	4
Probable	3
Poco probable	2
Improbable	1

Gravedad	
Descripción	Nivel
Extremadamente grave	5
Significativamente grave	4
Grave	3
Leve	2
Irrelevante	1

Los valores superiores de cada variable de riesgo (probabilidad y gravedad) señalan altos niveles de riesgo, que indican que estamos muy cerca de que se produzca la situación de riesgo y que las potenciales consecuencias son bastante graves.

La valoración del nivel de riesgo implica un cierto grado de subjetividad. En esta guía, aportamos unas orientaciones para reducir este margen de subjetividad, de acuerdo con unos criterios generales que ayuden a valorar el riesgo. El método de valoración de riesgos propuesto en esta guía es de tipo “semi cuantitativo”.

3.1 Valoración de la probabilidad

En cuanto a la probabilidad, utilizamos principalmente dos criterios de carácter general: por un lado, se debe tener en cuenta de qué manera las medidas previstas pueden reducir la probabilidad y por el otro, se debe considerar hasta qué punto el potencial escenario de riesgo se ha producido en otros tratamientos anteriormente.

Se pueden tener en cuenta otros criterios de valoración específicos de las operaciones de tratamiento, e incluso se pueden utilizar decimales si se quiere graduar más la valoración. Para esta graduación más detallada podemos tener en cuenta, por ejemplo, la eficacia de las medidas previstas de forma que, cuanto más eficaces sean, más cerca del nivel inferior tiene que estar la valoración final[51].

- **Una situación de riesgo es improbable** que se produzca cuando se han previsto varias medidas en forma de "línea de defensa", es decir, que si falla una siempre hay otra que continúa impidiendo los hechos no deseados.

  Otro criterio a tener en cuenta es si el hecho no deseado ya se ha producido con anterioridad, en proyectos similares del mismo responsable del tratamiento o en otras organizaciones. Si no se ha producido nunca (o no se sabe si se ha producido) y hay medidas interrelacionadas, consideramos improbable este potencial escenario de riesgo.

- **Una situación de riesgo es poco probable** que se produzca cuando se han previsto varias medidas en forma de "línea de defensa", es decir que si falla una hay otra que puede impedir el hecho no deseado, pero no en todos los casos.

  Si el hecho no deseado no se ha producido nunca (o no se sabe si se ha producido) y hay una interrelación parcial de las medidas, consideramos poco probable este potencial escenario de riesgo.

- **Una situación de riesgo es probable** que se produzca cuando las medidas para reducir la probabilidad no están previstas en forma de "línea de defensa", es decir que si falla una el resto no puede impedir el hecho no deseado.

  Si se conoce algún caso en que se ha producido el hecho no deseado y no hay interposición de las medidas, consideramos probable este potencial escenario de riesgo.

- **Una situación de riesgo es muy probable** que se produzca cuando se ha previsto una única medida para reducir su probabilidad y se conoce algún caso en

[51] El anexo 3 de la ISO/IEC 29134 (A.3) orienta de una manera sintética en cómo hacer la estimación de la probabilidad

que se ha producido el hecho no deseado. La suma de estos dos factores hace muy probable este potencial escenario de riesgo.

- **Una situación de riesgo es inminente** que se produzca cuando no se ha previsto ninguna medida para reducir su probabilidad y se conocen varios casos en que se ha producido el hecho no deseado. La suma de estos dos factores nos hace considerar que, de forma inminente, las operaciones de tratamiento se pueden ver afectadas por este potencial escenario de riesgo.

3.2 Valoración de la gravedad

En cuanto a la gravedad, utilizaremos criterios relacionados con las características del impacto que puede tener el potencial escenario de riesgo que estamos valorando.

Cómo en el caso de la probabilidad, se pueden tener en cuenta otros criterios específicos de las operaciones de tratamiento, así como la eficacia de las medidas previstas; cuanto más eficaces sean, más cerca del nivel inferior tiene que estar la valoración final.

- **Una situación de riesgo es irrelevante** cuando no se deriva un daño o perjuicio material o moral para las personas afectadas, ni se las priva de sus derechos o libertades. Por lo tanto, las consecuencias se centran en deficiencias formales leves, con consecuencias prácticamente imperceptibles[52], habitualmente relacionadas con las obligaciones materiales del responsable del tratamiento que se pueden corregir con medidas de fácil implantación.

- **Una situación de riesgo resultará leve** cuando no se deriva un daño o perjuicio material o moral para las personas afectadas, ni se las priva de sus derechos o libertades. Por lo tanto, las consecuencias se centran en deficiencias materiales leves, con mínimas consecuencias[53], habitualmente relacionadas con las obligaciones materiales del responsable del tratamiento, que se pueden corregir con medidas de fácil implantación.

- **Una situación de riesgo resulta grave** cuando se puede derivar un daño o perjuicio material o moral para las personas afectadas, difícil de reparar o que las

[52] Incorporado en la versión 2.0 de esta guía
[53] Incorporado en la versión 2.0 de esta guía

puede privar de manera parcial de sus derechos o libertades. Por lo tanto, las consecuencias se centran en deficiencias de cumplimiento del RGPD relacionadas con las obligaciones, derechos o principios, que se pueden corregir implantando medidas o mejorando la eficacia de las medidas implantadas[54].

- **Una situación de riesgo es significativamente grave** cuando se puede derivar un daño o perjuicio material o moral para las personas afectadas, difícil de reparar o que las puede privar totalmente de sus derechos o libertades. Por lo tanto, las consecuencias se centran en deficiencias de cumplimiento del RGPD relacionadas con las obligaciones, derechos o principios, que se pueden corregir implantando nuevas medidas o mejorando las existentes[55], aunque implique una cierta dificultad para el responsable del tratamiento.

- **Una situación de riesgo es extremadamente grave** cuando se puede derivar un daño o perjuicio material o moral para las personas afectadas, imposible de reparar o que las puede privar totalmente de sus derechos o libertades. Por lo tanto, las consecuencias se centran en deficiencias de cumplimiento del RGPD relacionadas con las obligaciones, derechos o principios, para las cuales no hay medidas a implantar o, si hay, requieren unos esfuerzos desproporcionados del responsable del tratamiento.

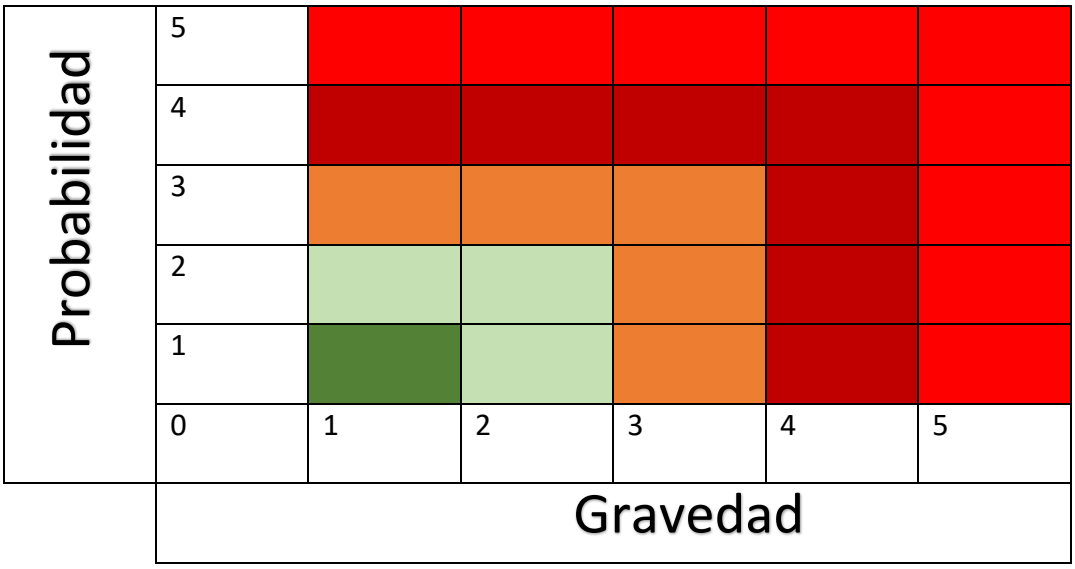
En la parte 3 de esta guía (modelo 7), se incluyen unas tablas resumen que pueden ser útiles para aplicar los criterios de valoración de los riesgos.

Una vez valorados todos los potenciales escenarios de riesgo, ya estamos en disposición de elaborar el mapa de riesgos inicial, que nos tiene que indicar en qué situaciones de riesgo es más urgente actuar. Podemos hacer esta valoración mediante una tabla similar a la que se ha utilizado para vincular los potenciales escenarios de riesgos a las medidas previstas, añadiendo la valoración del riesgo para cada PER (véase modelo 6 de la parte 3 de esta guía).

[54] Incorporado en la versión 2.0 de esta guía
[55] Incorporado en la versión 2.0 de esta guía

Mapa de riesgo inicial

Un mapa de riesgos es una representación visual o gráfica del nivel de riesgo en que se sitúa inicialmente el conjunto del tratamiento o un proceso clave concreto. Es una herramienta entre las diversas que ayudan a entender el riesgo y, por lo tanto, se puede elaborar de la manera más adecuada para la organización destinataria. Aquí se expone un ejemplo muy simple.



En lugar de hacer este mapa, se puede optar por utilizar únicamente tablas o la descripción textual de los diferentes niveles de riesgo del tratamiento.

Para determinar si los riesgos que presentan las operaciones de tratamiento son inaceptables, tolerables o aceptables, los niveles de riesgo se tienen que convertir a una segunda escala.

- Todos los potenciales escenarios de riesgo valorados con un nivel igual o superior a 3 se deben considerar riesgos inaceptables y, por lo tanto se deben aplicar medidas para reducir este nivel de riesgo, puesto que las operaciones de tratamiento estarían situadas en un nivel alto de riesgo.
- Cuando el nivel es igual a 2 el riesgo es tolerable, pero se tiene que incidir en la eficacia de las medidas previstas. Por lo tanto, conviene tratar estos riesgos para procurar bajarlos de nivel.

- Cuando el nivel se sitúa por debajo del valor 2 el riesgo es aceptable, puesto que los datos se están tratando en unas condiciones de riesgos razonablemente controlados. Debemos estar atentos a posibles variaciones de este riesgo y revisar la eficacia de las medidas que se implantan, pero desde el punto de vista de la EIPD no hay que tratarlos.

El nivel de riesgo global del tratamiento es el del potencial escenario de riesgo que tiene el nivel más alto de todos los que se han valorado. Por lo tanto, si un PER o un grupo de PER implica un riesgo inaceptable, el nivel de riesgo del tratamiento es inaceptable.

Esta primera estimación del nivel de riesgo se puede corregir aplicando otras valoraciones más subjetivas, adaptadas a las características concretas de las operaciones de tratamiento evaluadas y en relación al conjunto del tratamiento, por lo tanto se debe utilizar como una aproximación al nivel de riesgo[56].

Tratamiento de los riesgos iniciales

Si el resultado de la valoración de los riesgos es un riesgo inaceptable (riesgo alto), se deben diseñar medidas para situar estas operaciones de tratamiento en una zona de riesgo tolerable o aceptable.

Se tienen que seleccionar medidas nuevas o modificar y mejorar las previstas, y posteriormente volver a hacer el análisis y la valoración de los potenciales escenarios de riesgos, para verificar si los riesgos se han modificado y si ya podemos considerar que no están en zonas de riesgo alto.

Recordemos que si no podemos reducir el nivel de riesgo, y se mantiene alto, se tiene que hacer una consulta previa a la autoridad de protección de datos.

Al final, todo el proceso de gestión de riesgos se tiene que concretar en un informe de riesgos. En la parte 3 de esta guía, se aporta una propuesta de índice de este informe (modelo 8).

[56] Incorporado en la versión 2.0 de esta guía

INFORME DE EVALUACIÓN: CONCLUSIONES Y RECOMENDACIONES PARA MITIGAR LOS RIESGOS DE LAS OPERACIONES DE TRATAMIENTO

El informe final de la evaluación de impacto es la base para implantar las medidas encaminadas a mitigar los riesgos del tratamiento.

El destinatario principal de este informe es el responsable del tratamiento, que tiene que decidir cómo se tiene que modificar el diseño del proyecto para dar respuesta a la situación y a las recomendaciones derivadas de la EIPD. Pero la EIPD también puede tener como destinatarias a las personas afectadas por los tratamientos, no a título individual sino de manera colectiva, o incluso a la opinión pública en general, si el tratamiento es bastante relevante.

Si una vez realizada la evaluación de impacto se concluye que los tratamientos implican un alto riesgo, tenemos que plantear una consulta previa a la autoridad de control y entregarle buena parte de la documentación que se ha elaborado durante el proceso de evaluación. Por lo que, la autoridad de control es otra potencial destinataria del informe final de evaluación de impacto.

El documento final que recoge la evaluación de impacto tiene que transmitir con claridad que se ha tenido en cuenta el contenido mínimo que exige el artículo 35.7 del RGPD. El RGPD no prevé un informe concreto, de forma que la necesidad de documentar el proceso de evaluación se deriva del principio de responsabilidad proactiva.

En definitiva, se trata de integrar en un solo documento todo lo que hemos hecho para evaluar el impacto de las operaciones de tratamiento y las conclusiones y recomendaciones para minimizar los riesgos inherentes al tratamiento.

En la parte 3 de esta guía, se incluye una propuesta de índice de contenidos del informe de evaluación de impacto (véase modelo 9). Resulta conveniente mantener un registro de las EIPD realizadas y de su revisión; como ya se ha sugerido en esta guía se puede utilizar el registro de actividades de tratamiento para mantener un histórico de las evaluaciones realizadas.

Por otro lado, a partir del informe de evaluación de impacto se puede elaborar otro documento, para difundirlo entre las personas afectadas o a la opinión pública. Esta es una práctica muy extendida en los procesos de privacy *impact assessment* (PIA).

Informe público de evaluación de impacto[57]

El RGPD no prevé la obligación de hacer público el informe de evaluación, ni totalmente ni parcialmente. Pero hacerlo, puede resultar eficaz para generar confianza en las personas afectadas directamente por el tratamiento y, en general, en la opinión pública; esta iniciativa también es adecuada para añadir transparencia al tratamiento que lleva a cabo el responsable del tratamiento. No se trata de hacer público el informe interno, que puede contener información que no es adecuado difundir, sino de hacer una versión especial para hacerla pública.

Hay que tener presente que este documento está dirigido a personas que no tienen por qué conocer ni los procesos de EIPD, ni en general las cuestiones tecnológicas o de orden jurídico que pueden rodear un tratamiento de datos de carácter personal. Por lo tanto, se debe redactar en un lenguaje claro y exento de tecnicismos innecesarios.

También conviene incluir una parte introductoria, de carácter general, para explicar en qué consiste una evaluación de impacto sobre los datos personales. La forma más sencilla son las preguntas y respuestas sobre lo más relevante del informe.

> En la parte 3 de esta guía, se incluye una propuesta de índice de contenidos del informe público de evaluación (véase modelo 10).

Habitualmente se accede a este informe público desde la página web del responsable del tratamiento, que debe permitir que de manera libre, sin solicitar ninguna identificación personal ni ningún otro requisito, que quién lo desee se pueda descargar el informe.

[57] El GT29 en las directrices del WP 248 recomienda hacer pública información sobre la EIPD

SUPERVISIÓN Y REVISIÓN DE LA EVALUACIÓN DE IMPACTO

El informe final de la evaluación de impacto es la base para implantar las medidas encaminadas a mitigar los riesgos del tratamiento y es útil para verificar que, efectivamente, las medidas se han implantado tal como se han definido en la EIPD.

Una vez iniciado el tratamiento se debe revisar si las previsiones de impacto iniciales continúan siendo válidas, o si ha habido cambios sustanciales que afectan a las operaciones de tratamiento. De hecho, como ya sabemos, el tratamiento en su inicio era de riesgo alto, por lo tanto, deberá ser objeto de especial monitorización por parte del responsable del tratamiento, y de especial supervisión por parte de delegado de protección de datos[58].

Tal como se propone en esta guía, el informe final de evaluación de impacto tiene que incluir un apartado específico que recoja cómo se ha previsto revisar la evaluación de impacto, tanto de manera ordinaria como extraordinaria (véase modelo 9, apartado anexos).

Implantación y seguimiento de las recomendaciones

La evaluación de impacto identifica las diferentes medidas que se han previsto, ya sea inicialmente o como una actuación correctiva.

> Se debe prever mecanismos para controlar que las medidas recogidas en la evaluación de impacto se han implantado. Por lo tanto, se deben establecer responsabilidades respecto de cómo se implantan.

Las EIPD son especialmente útiles en la fase de diseño del tratamiento, cuando el sistema todavía no se ha construido, puesto que es el momento de introducir las medidas derivadas de la evaluación de impacto. Por lo tanto, se debe verificar tanto este diseño final como su implantación.

El delegado de protección de datos (si lo hay) tiene que asesorar durante el proceso de evaluación de impacto. Lo más recomendable es que también participe en la fase

[58] Incorporado en la versión 2.0 de esta guía

de implantación de las medidas, para poder supervisar que se implantan correctamente.

Cuando el artículo 39.1.*c)* del RGPD define las funciones del delegado de protección de datos, indica que debe ofrecer el asesoramiento que se le pida sobre la evaluación de impacto relativa a la protección de datos, y supervisar su aplicación.

Revisión de la evaluación

Una vez se ha implantado el sistema de acuerdo con lo que prevé la EIPD y se han supervisado las medidas, se pueden iniciar las operaciones de tratamiento.

Aun así, tenemos que recordar que se consideró que, en conjunto, las operaciones de tratamiento entraban dentro de los supuestos que hacían necesaria la evaluación de impacto, puesto que implicaban unos riesgos inherentes relevantes para la protección de los datos de carácter personal (alto riesgo, en general).

Se debe revisar el tratamiento periódicamente, para verificar que los riesgos están controlados.

Se tienen que prever dos tipos de revisiones: ordinarias y extraordinarias.

- Para las ordinarias, la periodicidad adecuada es cada dos o tres años, en todo caso se trata de una decisión que debe tomar el responsable del tratamiento a la vista de las particularidades y riesgo que potencialmente implica el tratamiento[59], por lo tanto, no se pueden descartar otros plazos en función de esas particularidades.

  La revisión ordinaria es un proceso muy similar al de una auditoría: tenemos un modelo de referencia (la evaluación de impacto) que tenemos que comparar con la realidad (el tratamiento y las medidas implantadas). Por eso, no se tiene que volver a ejecutar una evaluación de impacto completa, sino que se debe verificar que no han aparecido riesgos nuevos, que los ya conocidos se mantienen en el mismo nivel y que las medidas implantadas continúen siendo adecuadas.

[59] Incorporado en la versión 2.0 de esta guía

- Las revisiones extraordinarias se tienen que hacer cuando las operaciones de tratamiento se modifican sustancialmente, porque se introducen nuevas tecnologías, nuevas finalidades, nuevos datos, nuevos afectados, etc.

  En este caso, es conveniente hacer una evaluación de impacto más completa, para actualizar la evaluación inicial de acuerdo con los cambios relevantes que se han producido en las condiciones del tratamiento.

PARTE 3

Modelos de documentos de trabajo

Modelo 1. Plantillas de recogida de información sobre los datos y operaciones de tratamiento (la información entre los símbolos *[…]* hay que sustituirla por la que corresponda y se pueden añadir otras observaciones)

Este es un documento de trabajo[60] orientado a recoger y sistematizas la información relacionada con los datos que se tienen que tratar y sobre las operaciones de tratamiento que se quieren llevar a cabo.

En esta etapa previa a la EIPD, la información recogida es relevante para determinar si hay un tratamiento de datos de carácter personal para el cual es obligatorio hacer la evaluación de impacto. Pero también será útil posteriormente, si se hace la EIPD, en la fase de descripción del proyecto y de los flujos de información.

Conviene hacer una breve memoria descriptiva del proyecto, a la cual se puede añadir el resultado de aplicar estas plantillas de recogida de información.

Se tienen que identificar y clasificar todos los datos de carácter personal que se prevén tratar. Hay que insistir que aquí se presentan unos modelos de documentos de trabajo orientativos, que se pueden adaptar y mejorar.

[60] En la versión 2.0 se han simplificado y unificado los formularios que se incluyeron en este apartado de la versión 1.0 de la guía

Recogida de información sobre los datos y operaciones de tratamiento			
[Identificación del tratamiento]			
CLASE A. Datos de carácter personal facilitados directamente por las personas afectadas			
		Dato de categoría especial	
Código	Descripción	SI	NO
[A.1]	[DATO1] (por ejemplo: DNI)	[X]	
[A.2]	Etc.		[X]
CLASE B. Datos de carácter personal facilitados por terceros (el origen de los datos son cesiones o comunicaciones)			
Código	Descripción	SI	NO
[B.1]	[DATO2] (por ejemplo: apellidos)		
[B.2]	Etc.		
CLASE C. Datos de carácter personal ya disponibles anteriormente (el origen de los datos es el propio responsable del tratamiento, que dispone de estos datos porque los ha tratado previamente)			
Código	Descripción	SI	NO
C.1	[DATO1] (Por ejemplo: histórico altas y bajas)		
C.2	Etc.		
CLASE D. Datos de carácter personal capturados (los datos se han obtenido mediante dispositivos o aplicaciones que de manera autónoma, sin una acción concreta de la persona afectada, recogen información diversa –información de "cookies", navegador utilizado, información de dispositivos móviles, coordenadas de geoposicionamiento, dirección IP, tiempo de conexión, etc.			
Código	Descripción	SI	NO
D.1	[DATO1] (por ejemplo: dirección IP)		
D.2	Etc.		
CLASE E. Datos de carácter personal calculados (el origen son operaciones de tratamiento que dan como resultado información de carácter personal adicional: coordenadas de geoposicionamiento que es traducen en ubicaciones concretas, preferencias de consumo, nivel de riesgo financiero, etc.)			
Código	Descripción	SI	NO
E.1	[DATO1] (por ejemplo: distancia)		
E.2	Etc.		
CLASE Z. Datos que inicialmente no se considera dato de caràcter personal (esta clasificación puede variar posteriormente: direcciones IP, versiones de navegador, datos anonimizados, etc.)			
Código	Descripción	SI	NO
Z.1	[DATO1] (por ejemplo: código de seudonimización)		
Z.2	Etc.		

Breve descripción de las operaciones de tratamiento
Se trata de hacer una descripción genérica de las operaciones de tratamiento más relevantes, a título orientativo conviene hacer referencia a: a) La finalidad del tratamiento b) Los mecanismos de recogida de los datos (por ejemplo: formulario web). c) El sistema de almacenamiento (por ejemplo: base de datos situada en un servicio en la nube). d) Los usos principales que se tiene previsto dar a los datos (por ejemplo: la identificación del titular de los datos). e) La previsión de volumen de personas afectadas por el tratamiento f) Si es posible, la previsión de los plazos de conservación de los datos g) El alcance geográfico de los tratamientos h) Si se utilizarán tecnologías emergentes o especialmente intrusivas en la intimidad o privacidad de las personas Se pueden añadir otras informaciones relevantes para la EIPD.
Breve descripción de los colectiuvos de personas afectadas por el tratamiento
Hay que indicar, particularmente, si se prevé tratar datos de niños, o de personas en situación de vulnerabilidad, o en otras circunstancias de desequilibrio respecto del responsable de tratamiento, que pueden evidenciar situaciones especiales que requieren que los datos de carácter personal se traten con especial cautela. Conviene tener en cuenta si el tratamiento de estos datos puede ser incidental.

Modelo 2. Listas de verificación

Estas listas de verificación son una orientación de método de trabajo, y tienen como objetivo sistematizar el proceso de análisis de la necesidad de hacer la EIPD. No son listas cerradas, sino que se pueden ampliar de acuerdo con las diferentes casuísticas de tratamientos para las cuales se usen.

Elementos a analizar	SÍ	NO
¿La autoridad de supervisión competente ha publicado una lista de tratamientos para los cuales se debe hacer la evaluación de impacto? **Responder sólo en caso afirmativo.** ¿El tratamiento objeto de evaluación se puede considerar incluido en esta lista?		
¿La autoridad de supervisión competente ha publicado una lista de tratamientos que no se deben evaluar? **Responder sólo en caso afirmativo.** ¿Consideramos que el tratamiento no encaja claramente en ninguno de los supuestos de la lista?		
¿Las operaciones de tratamiento implican una evaluación sistemática y amplia de aspectos personales relativa a personas físicas?		
¿Con las operaciones de tratamiento, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables?		
A todos los efectos, ¿podemos considerar que una de las finalidades del tratamiento es elaborar perfiles personales o predecir comportamientos?		
A partir del tratamiento de los datos, ¿se toman decisiones con efectos jurídicos para las personas afectadas?		
A partir del tratamiento de los datos, ¿se toman decisiones que pueden afectar significativamente o perjudicar de alguna manera las personas afectadas?		
¿Se tratan datos a gran escala de alguna categoría especial?		
¿Se tratan datos relativos a condenas o infracciones penales[61]?		
¿El tratamiento implica un control sistemático, monitorización o supervisión a gran escala de áreas de acceso público?		

Si alguna de las respuestas es “SI”, muy probablemente estaremos ante un tipo de tratamiento de los previstos en el artículo 35.3 del RGPD y por tanto habrá que hace la EIPD[62].

[61] Incorporado en la versión 2.0 de esta guía

Elementos complementarios a analizar	SÍ	NO
¿La iniciativa o proyecto supone recoger datos de carácter personal que hasta ahora no se recogían?		
¿La iniciativa implica relacionar diferentes fuentes u orígenes de datos personales (cruzar información), que de alguna manera incrementen la capacidad de análisis de la información?		
¿La información se ha sometido a un proceso de disociación o seudoanonimización?		
¿Los datos personales se comunicarán a organizaciones o personas que anteriormente no han tenido acceso?		
¿Se prevé utilizar información personal de la que se dispone, para finalidades o usos diferentes a los previstos inicialmente?		
¿La iniciativa que se tiene que evaluar implica el uso de tecnologías que se pueden percibir como especialmente intrusivas para la privacidad?		
¿Hay riesgos específicos para la seguridad de la información, especialmente un riesgo relevante de que terceros no autorizados accedan?		
¿Se han previsto transferencias internacionales de datos?		
Indicar el país importador de los datos (pueden ser varios):		
¿Se tratan datos de personas menores de 18 años?		
¿Se tratan datos de personas menores de [14] años?		

Estas preguntas, y el análisis de las respuestas, nos permiten detectar cuestiones que si bien de forma aislada tal vez tendrían una incidencia directa en la decisión de hacer la EIPD, su valoración conjunta quizás si que nos lleva a considerar que estamos ante un tratamiento que supone un alto riesgo[63].

[62] Incorporado a la versión 2.0 de esta guía
[63] Incorporado a la versión 2.0 de esta guía

Existencia de factores de riesgo (criterios del WP 248) [64]	SÍ	NO
¿El tratamiento implica la evaluación o puntuación de personas?		
¿El tratamiento implica elaborar perfiles de personas o hacer predicciones sobre su comportamiento?		
¿La finalidad del tratamiento es tomar decisiones de manera automatizada, que puedan tener efectos jurídicos?		
¿La finalidad del tratamiento es tomar decisiones de manera automatizada, que puedan tener efectos similares a los jurídicos, o efectos significativos para las personas?		
¿El tratamiento implica algún tipo de vigilancia sistemática? (observación, supervisión y control de personas)		
¿Se tratan categorías especiales de datos?		
¿Se tratan datos relativos a condenas o infracciones penales?		
¿Se traten datos que es puedan considerarse como muy personales?		
¿Se tratan datos a gran escala?		
¿El tratamiento implica combinar diferentes fuentes de información o datos relacionados con tratamientos diversos?		
¿Se tratan datos relativos a personas en situación de vulneración o de desequilibrio respecto del responsable del tratamiento?		
¿Se tratan datos de niños? (personas menores de 18 años)		
¿Las operaciones de tratamiento utilizan o aplican soluciones tecnológicas u organizativas de forma innovadora?		
¿El tratamiento puede impedir a las personas afectadas utilizar un servicio o ejecutar un contrato?		

[64] Modificada en la versión 2.0 de la guía. Esta lista se ha adaptado a la versión revisada de los criterios del WP 248

Modelo 3. Índice de contenidos del informe del análisis de la necesidad de hacer la evaluación de impacto

Este índice es orientativo respecto de los contenidos que, como mínimo, es conveniente que formen parte de un informe sobre el proceso de valoración de la obligación de hacer una evaluación de impacto de un tratamiento de datos de carácter personal. En definitiva, recoge el resultado de las diferentes tareas de análisis que se han hecho y concluye con la decisión sobre si hay que hacer la EIPD. Esta decisión debe estar argumentada y debe quedar registrada[65].

1. Descripción del proyecto
    - 1.1 Promotor del proyecto
    - 1.2 Funcionalidades previstas e implantación
    - 1.3 Personas o grupos de personas afectadas
    - 1.4 Sistemas de información y tecnologías
    - 1.5 [Otras informaciones]

2. Identificación y clasificación de los datos
    - 2.1 Respecto de los datos objeto de tratamiento
    - 2.2 [Otras cuestiones relativas a los datos]

3. Operaciones de tratamiento
    - 3.1 Respecto de las operaciones de tratamiento
    - 3.2 [Otras cuestiones relativas a las operaciones de tratamiento]

4. Análisis de la necesidad de hacer la evaluación de impacto

5. Identificación y consulta a las personas afectadas por los tratamientos[66]
    - 5.1 Personas y grupos afectados
    - 5.2 Conveniencia de informar y consultar
    - 5.3 Gestión de la consulta/información a las partes afectadas

6. Conclusiones y recomendaciones

7. Anexos

[65] Modificado en la versión 2.0 de la guía. En esta guía se propone que una opción para mantener el registro de las EIPD podría ser su incorporación al registro de actividades de tratamiento previsto en el artículo 30 del RGPD

[66] En el caso de que la EIPD sea obligatoria

Modelo 4[67]. Índice de contenidos del documento que describe de manera sistemática las operaciones de tratamiento

Este índice es orientativo respecto de los contenidos que, como mínimo, es conveniente que formen parte de un documento que describa de una manera sistemática las operaciones de tratamiento.

1. Identificación del proyecto
    - 1.1 Nombre o acrónimo que identifica el proyecto
    - 1.2 Entidad o entidades promotoras
    - 1.3 Entidad o entidades participantes
    - 1.4 Responsabilidades en el proyecto
    - 1.5 Antecedentes

2. Objetivos y finalidades que persigue
    - 2.1 Finalidad del tratamiento
    - 2.2 Legitimación de las operaciones de tratamiento
    - 2.3 Necesidad y proporcionalidad de las operaciones de tratamiento
    - 2.4 Personas o colectivos afectados

3. Descripción del ciclo de vida de la información
    - 3.1 Entrada
    - 3.2 Almacenamiento
    - 3.3 Acceso
    - 3.4 Supresión

4. Análisis por capas
    - 4.1 Procesos clave
    - 4.2 Modelo conceptual de datos
    - 4.3 Intervinientes
    - 4.4 Flujo de información
    - 4.5 Tecnologías

5. Anexos

[67] En la versión 2.0 de la guía se ha modificado el apartado 3 de este modelo

Modelo 5. Lista base de potenciales escenarios de riesgo

Escenarios de riesgo que pueden afectar a los principios	
Código	Descripción
RP1	La base que legitima el tratamiento no es adecuada, es ilícita o no se ha formalizado adecuadamente (se debe prestar atención a las categorías especiales de datos y a la gestión del consentimiento)
RP2	Si el tratamiento se basa en el interés legítimo: no se ha ponderado adecuadamente este interés legítimo en relación con los intereses, derechos y libertades fundamentales del interesado
RP3	Las finalidades del tratamiento no son precisas, son ilegítimas, etc.
RP4	Hay un cambio de finalidad que puede ser incompatible con la finalidad original
RP5	Hay un cambio de finalidad compatible, pero puede invalidar una evaluación de impacto previa
RP6	Se recogen datos inadecuados, no pertinentes, excesivos o innecesarios para la finalidad prevista
RP7	Se registran datos inexactos o no se mantienen actualizados
RP8	Los datos personales se conservan más tiempo del necesario
RP9	Los datos se tratan de manera desleal o poco transparente (no se cumple la expectativa de la persona interesada respecto del tratamiento de sus datos)
RP10	Se hacen operaciones de tratamiento desproporcionadas
etc.	…

Escenarios de riesgo que pueden afectar a los derechos	
Código	Descripción
RD1	En el momento de la recogida de los datos no se proporciona la información mínima prevista a la persona afectada (cuando los datos se obtienen directamente de la persona) o no se le proporciona ninguna información, cuando se obtienen de terceros
RD2	La respuesta al ejercicio del derecho de acceso no se hace en el tiempo y la forma adecuados
RD3	La respuesta al ejercicio del derecho de rectificación no se hace en el tiempo y la forma adecuados
RD3	La respuesta al ejercicio del derecho de supresión no se hace en el tiempo y la forma adecuados
RD4	La respuesta al ejercicio del derecho a la limitación del tratamiento no se hace en el tiempo y la forma adecuados
RD5	La respuesta al ejercicio del derecho de portabilidad de los datos no se hace en el tiempo y la forma adecuados
RD6	La respuesta al ejercicio del derecho de oposición no se hace en el tiempo y la forma adecuados
RD7	Se toman decisiones que afectan a una persona utilizando exclusivamente medios automatizados
RD8	No hay procedimientos para dar una respuesta adecuada a los derechos

RD9	La organización desconoce los procedimientos para responder el ejercicio de derechos
RD10	No se verifica adecuadamente la identidad de la persona que ejerce un derecho
etc.	…

Escenarios de riesgo que pueden afectar a las obligaciones	
Código	Descripción
R.O.1	Se incumple la regulación general sobre el derecho a la protección de los datos de carácter personal
R.O.2	Se incumplen otras regulaciones sectoriales que inciden en la protección de los datos de carácter personal
R.O.3	Se incumplen las cláusulas sobre la protección de datos incorporados a los contratos o condiciones de uso
R.O.4	Se incumplen estipulaciones recogidas en un código de conducta (si se está adherido)
R.O.5	No se puede demostrar el cumplimiento (responsabilidad proactiva)
R.O.6	Las certificaciones o sellos de protección de datos no se han renovado o han perdido vigencia
R.O.7	No se ha tenido en cuenta la protección de datos en el momento de diseñar el tratamiento (de manera parcial o total)
R.O.8	No se ha incorporado la protección de datos por defecto en las operaciones de tratamiento (de manera parcial o total)
R.O.9	No se ha hecho una consulta previa a la autoridad de supervisión, cuando era necesaria
R.O.10	Los encargados de tratamiento no se han seleccionado adecuadamente
R.O.11	No se ha formalizado adecuadamente la relación con los encargados de tratamientos
R.O.12	No se ejerce suficiente control sobre la actividad del encargado de tratamiento (en las operaciones de tratamiento que le han sido encargadas)
R.O.13	Se desconocen las cadenas de subcontratación de los encargados de tratamiento
R.O.14	No se dispone del registro de actividades de tratamiento (si es obligatorio)
R.O.15	No se mantiene actualizado (no se gestiona) el registro de actividades de tratamiento.
	Seguridad de los tratamientos
R.O.16	Hay destrucción accidental de datos personales
R.O.17	Hay destrucción malintencionada de datos personales
R.O.18	Hay perdida de datos personales
R.O.19	Hay alteración no autorizada de datos personales
R.O.20	Hay comunicación no autorizada de datos personales
R.O.21	Hay acceso no autorizado a datos personales
R.O.22	Los sistemas de información no están disponibles (incidente que provoca que los datos personales no estén disponibles)
R.O.23	Hay incapacidad para detectar y gestionar incidentes que afectan a la seguridad de los datos

R.O.24	Las violaciones de datos no se notifican en el tiempo y la forma adecuados (*data breach*)
R.O.25	Las violaciones de datos no se comunican en el tiempo y la forma adecuados (*data breach)*
R.O.26	Las limitaciones del tratamiento no se comunican a terceros
R.O.27	Hay transferencia internacional de datos no autorizada o desconocida
R.O.28	No se ha designado delegado de protección de datos (si es obligatorio)
R.O.29	No se proporcionan medios suficientes al delegado de protección de datos
R.O.30	No se atiende un requerimiento de la autoridad de supervisión competente
R.O.31	No se hace la evaluación de impacto (si es obligatoria)
R.O.32	No se implantan las medidas derivadas de una evaluación de impacto
R.O.34	No se atiende a las instrucciones de una autoridad de protección de datos
R.O.35	No se verifican las medidas adoptadas (auditoría de cumplimiento)
etc.	…

Escenarios de riesgo que pueden afectar a otros derechos y libertades	
Código	Descripción
RDL1	Vulneración de la imagen, la intimidad o el honor de las personas
RDL2	Vulneración del libre desarrollo de la personalidad
RDL3	Discriminación por razón de sexo, raza, religión, opinión, etc.
RDL4	Violación del secreto de las comunicaciones
RDL5	Atentado contra la dignidad de las personas
etc.	…

Escenaris de risc que poden causar directament daños y perjuicios[68]	
Codi	Descripció
RDP1	Discriminar a una persona en un proceso competitivo
RDP2	Discriminar a un colectivo
RDP3	Impacto económico negativo
RDP4	Peligro para la integridad física o salud
RDP5	Suplantación de la identidad
RDP6	Perjudicar a la reputación
RDP7	Prohibir el acceso físico
RDP8	Impedir o denegar la obtención de un servei
RDP9	Impedir una contratación
RDP10	Denegar una ayuda o ventaja
etc.	…

[68] Tabla incorporada en la versión 2.0 de esta guía

Modelo 6. Tablas de ejemplo para el análisis y valoración de los riesgos

ANÁLISIS DE RIESGOS			
Proceso clave: [...]		MEDIDAS PREVISTAS INICIALMENTE	
Potenciales escenarios de riesgo		REDUCIR PROBABILIDAD	REDUCIR GRAVEDAD
[código]	[...]	[...]	[...]
		[...]	[...]
		[...]	
[código]	[...]	[...]	n/p[69]

VALORACIÓN DE RIESGOS					
Proceso clave: [...]		NIVEL INICIAL DE RIESGO			
Potenciales escenarios de riesgo		PROBABILIDAD		GRAVEDAD	
[código]	[...]	[nivel]	[valor numérico]	[nivel]	[valor numérico]
[código]	[...]	[nivel]	[valor numérico]	[nivel]	[valor numérico]

[69] No se han previsto

Modelo 7. Tablas resumen de los criterios de valoración de la probabilidad y la gravedad.

Estas tablas resumen los criterios que facilitan la valoración de los riesgos de las operaciones de tratamiento, tanto en relación a la probabilidad como la gravedad.

	PROBABILIDAD				
	Improbable	**Poco probable**	**Probable**	**Muy probable**	**Inminente**
Se han previsto varias medidas	●	●			
Se han previsto algunas medidas			●		
Se ha previsto una única medida				●	
No se ha previsto ninguna medida					●
Todas las medidas forman línea de defensa	●				
Algunas medidas forman línea de defensa		●			
Las medidas no forman línea de defensa			●		
El hecho no deseado no se ha producido nunca antes	●	●			
El hecho no deseado se ha producido antes			●	●	
El hecho no deseado se ha producido varias veces antes					●

	GRAVEDAD				
	Irrelevante	**Leve**	**Grave**	**Significativamente grave**	**Extremadamente grave**
No se deriva ningún daño ni perjuicio	●	●			
Se deriva algún daño o perjuicio			●	●	●
Es difícil reparar el daño o perjuicio			●	●	
Es imposible reparar el daño o perjuicio					●
No hay privación de derechos o libertades	●	●			
Hay privación parcial de derechos y libertades.			●	●	
Hay privación total de derechos y libertades.					●
Implica una deficiencia formal leve	●				
Implica una deficiencia material leve		●			
Se incumplen obligaciones materiales	●	●			
Se incumplen obligaciones, derechos y principios.			●	●	●
Hay medidas que se pueden implantar fácilmente	●	●			
Se pueden implantar medidas			●		
Hay medidas difíciles de implantar				●	
Hay medidas que requieren esfuerzos desproporcionados					●
No hay medidas					●

Modelo 8. Índice de contenidos del informe de gestión de riesgos

Este índice es orientativo de los contenidos que tienen que formar parte de un documento que describe e informa sobre cómo se ha hecho la gestión de riesgos del tratamiento.

1. Breve contextualización del proyecto

2. Objeto y alcance de la gestión de riesgos que se ha hecho

3. Metodología de gestión de riesgos que se ha utilizado

4. Potenciales escenarios de riesgo
    - 4.1 Medidas previstas inicialmente
    - 4.2 Estimación del nivel de riesgo inicial
    - 4.3 Medidas propuestas para tratar el riesgo inicial
    - 4.4 Influencia de las medidas propuestas
    - 4.5 Estimación del nivel de riesgo residual

5. Análisis del cumplimiento normativo y medidas para demostrar el cumplimento[70]
[si es considera la conveniencia de tratar el cumplimiento normativo aparte)

6. Conclusiones y recomendaciones

7. Anexos

[70] Incorporado en la versión 2.0 de esta guía

Modelo 9. Índice de contenidos del informe de evaluación de impacto

Este índice es orientativo de los contenidos que tienen que formar parte del informe final de evaluación de impacto.

1. Identificación del proyecto

1.1 Nombre

1.2 Descripción breve

1.3 Responsables del proyecto y datos de contacto

1.4 Equipo de evaluación (quién ha hecho la evaluación de impacto)

1.5 Fecha del informe

1.6 Versión del informe

2. Resumen ejecutivo

2.1 Descripción ejecutiva del proyecto

2.2 Descripción del método de evaluación (descripción breve de cómo se ha hecho la evaluación, calendario, etapas, etc.)

2.3 Principales riesgos que se han identificado

2.4 Resumen de las medidas más relevantes que se han propuesto para mitigar los riesgos

2.5 Medidas que afectan los encargados de tratamiento.

2.6 Necesidad de hacer una consulta previa

3. Análisis de la necesidad de la evaluación (se tiene que trasladar el análisis de necesidad que se ha realizado)

3.1 Resultado del análisis

3.2 Motivación de la necesidad de hacer la EIPD

4. Descripción detallada del proyecto (se tienen que trasladar los contenidos del informe de descripción sistemática del tratamiento)

4.1 Descripción del tratamiento

4.2 Descripción detallada

4.3 Necesidad y proporcionalidad de las operaciones de tratamiento

5. Resultado del proceso de consultas (si procede)

5.1 Identificación de las partes interesadas (internas y externas).

5.2 Mecanismo de consulta y contribuciones de las partes

5.3 Resumen de los aspectos más relevantes derivados de la consulta

6. Identificación y gestión de riesgos (se tienen que trasladar los contenidos del informe de gestión de riesgos)

6.1 Identificación detallada de riesgos

6.2 Impacto y probabilidad de cada riesgo identificado

6.3 Gestión de los riesgos

6.4 Análisis de cumplimiento normativo (si es relevante, hay que segregarlo de la gestión de riesgos y deben añadirse las medidas orientadas a demostrar el cumplimiento[71])

7. Conclusiones

7.1 Análisis final

7.2 Recomendaciones

7.3 Resumen de medidas a implantar

8. Anexos

8.1 Proceso de implantación de las medidas propuestas

I. Organización

II. Verificación

III. Monitorización

8.2 Revisión de la evaluación de impacto

I. Ordinaria

II. Extraordinaria

8.3 Conceptos y definiciones.

[71] Incorporado en la versión 2.0 de esta guía

Modelo 10. Índice de contenidos del informe público de evaluación de impacto

Este índice es orientativo de los contenidos que pueden formar parte del informe público de evaluación de impacto.

1. Introducción

1.1 ¿Qué es una evaluación de impacto?

1.2 ¿Qué utilidad tiene?

1.3 ¿Cuándo hay que hacerla?

1.4 ¿Quién la tiene que hacer?

1.5 [otros]

1.6 Conceptos y definiciones.

2. Descripción del proyecto evaluado

2.1 Responsables del tratamiento

2.2 Operaciones de tratamiento más relevantes

2.3 Datos tratados

2.4 Motivos por los cuales se ha hecho la evaluación

3. Consultas a terceros

3.1 Partes afectadas

3.2 Autoridad de supervisión

4. Gestión de los riesgos

4.1 Situaciones de riesgo evaluadas

4.2 Decisiones tomadas para minimizar los riesgos

5. Datos de contacto para obtener más información