RGPD

Informe de Evaluación de Impacto relativa a la protección de datos

GENETRACER BIOTECH

EVALUACIÓN DE LOS RIESGOS INHERENTES A LA ACTIVIDAD DESARROLLADA POR LA ENTIDAD Y PROPOSICIÓN DE MEDIDAS MITIGADORAS DEL MISMO

CUMPLIMIENTO CON LO ESTABLECIDO EN EL ART. 35 DEL REGLAMENTO (UE) 2016/679 (RGPD) Y ART. 28 DE LA LEY ORGÁNICA 3/2018

REALIZACIÓN DE LA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (EIPD)

De conformidad con lo señalado en el considerando 84 del Reglamento general de protección de datos, en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el citado Reglamento.

En su consecuencia, el responsable del tratamiento GENETRACER BIOTECH, S.L. ha realizado, con fecha de emisión 23/03/2022, una evaluación de impacto relativa a la protección de datos, con la finalidad de dar cumplimiento con lo establecido en el artículo 35, apartado 1, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016) (RGPD):

> *Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.*

Así mismo, la citada evaluación de impacto en la protección de datos se ha realizado en cumplimiento de lo establecido en el artículo 28, apartado 1, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, 06-12-2018) (LOPDGDD), que tiene por objeto adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679:

> *Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.*

De acuerdo a lo señalado en las Directrices del Grupo de Trabajo sobre protección de datos del artículo 29 (GT29) sobre la evaluación de impacto relativa a la protección de datos (EIPD), la EIPD es un proceso continuo, especialmente cuando una operación de tratamiento es dinámica y está sujeta a cambios permanentes.

En tal sentido, la actualización de la EIPD a lo largo del ciclo de vida del proyecto o de las operaciones de tratamiento garantizará que se tenga en cuenta la protección de los datos y la intimidad y propiciará la creación de soluciones que fomenten el cumplimiento.

También puede resultar necesario repetir pasos concretos de la evaluación a medida que avance el proceso de desarrollo del proyecto o de las operaciones de tratamiento debido a que la selección de determinadas medidas técnicas u organizativas puede afectar a la gravedad o probabilidad de los riesgos que suponga el tratamiento.

ÍNDICE

II. EVALUACIÓN DE LA NECESIDAD Y PROPORCIONALIDAD DEL TRATAMIENTO

- **FASE 4: IDENTIFICACIÓN DE AMENAZAS**
- **FASE 5: RIESGO INHERENTE**
- **FASE 6: PLAN DE ACCIÓN**
- **FASE 7: RIESGO RESIDUAL ESPERADO Y CONSULTA PREVIA**
- **RESUMEN EJECUTIVO DE LA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (EIPD)**

NORMATIVA APLICABLE

- Directrices del Grupo de Trabajo sobre protección de datos del artículo 29 (GT29) sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679. Adoptadas el 4 de abril de 2017. Revisadas por última vez y adoptadas el 4 de octubre de 2017.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, 06-12-2018) (LOPDGDD).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016) (RGPD).

IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO

El siguiente responsable del tratamiento ha realizado una evaluación de impacto relativa a la protección de datos, con la finalidad de dar cumplimiento con lo establecido en el artículo 35 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016) (RGPD), y en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, 06-12-2018) (LOPDGDD):

a) Nombre y datos de contacto del responsable del tratamiento:

- Nombre y apellidos / Denominación: GENETRACER BIOTECH S.L.
- NIF: B39758370
- Teléfono de contacto: 679152601
- Domicilio profesional / Domicilio social: C/ Isabel Torres 11, CP 39011 - Santander
- Domicilio a efecto de notificaciones: Edificio de Oncología, planta 3. Hospital Universitario de Fuenlabrada. Camino del Molino 2. 28942 - Madrid
- Dirección electrónica de contacto: carlos.cortijo@genetracerbiotech.com
- Página web (URL): www.genetracerbiotech.com

b) Nombre y datos de contacto del delegado de protección de datos:

- Nombre y apellidos / Denominación: AUDIDAT 3.0, S.L.U.
- DPD Interno / Externo: Externo
- Teléfono de contacto: 967600975
- Dirección electrónica de contacto: dpd@audidat.com

ASESORAMIENTO TÉCNICO-JURÍDICO EN LA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (EIPD)

De conformidad con lo establecido en el artículo 35, apartado 1, del Reglamento (UE) 2016/679, y en el en el artículo 28, apartado 1, de la Ley Orgánica 3/2018, es el responsable del tratamiento quien debe garantizar que la evaluación de impacto relativa a la protección de datos se lleva a cabo. En tal sentido, cualquier otra persona, de dentro o fuera de la entidad, puede llevar a cabo una EIPD, pero el responsable del tratamiento sigue respondiendo en última instancia por la tarea realizada.

Señalado lo anterior, las Directrices del Grupo de Trabajo sobre protección de datos del artículo 29 (GT29) sobre la evaluación de impacto relativa a la protección de datos (EIPD), recomiendan «recabar el asesoramiento de expertos independientes (abogados, expertos en TI, expertos en seguridad, sociólogos, expertos en ética, etc.)» para la realización de la EIPD.

En su consecuencia, la evaluación de impacto relativa a la protección de datos objeto del presente informe ha sido realizada bajo el asesoramiento de la Dirección Técnico-Jurídica de AUDIDAT 3.0, S.L.U. (en adelante, también e indistintamente, AUDIDAT), entidad provista de CIF B02482545, y con domicilio a efectos de notificaciones en Calle Martínez Villena, 14, 3ª Planta, CP 02001, Albacete.

AUDIDAT 3.0, S.L.U. es una entidad de reconocido prestigio, comprometida con la calidad y la seguridad de la información, y con una dilatada experiencia en la prestación de servicios jurídicos especializados en materia de protección de datos, cabiendo citar los siguientes méritos preferentes:

- El sistema de gestión de la calidad de AUDIDAT 3.0, S.L.U. es conforme con la norma UNE-EN ISO 9001:2008.
- El sistema de gestión de la seguridad de la información de AUDIDAT 3.0, S.L.U. es conforme con la norma UNE-ISO/IEC 27001:2014.
- AUDIDAT 3.0, S.L.U. es empresa asociada de la Asociación para el Fomento de la Seguridad de la Información ISMS FORUM.
- AUDIDAT 3.0, S.L.U. dispone de un equipo de delegados de protección de datos certificados, de conformidad con el «Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD)».

OBJETO DEL INFORME

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

En este sentido, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016) (RGPD), establece un marco sólido y coherente para la protección de datos en la Unión Europea, reforzando la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas.

En España, la protección de datos personales también es un derecho fundamental de las personas físicas consagrado en la Sentencia 292/2000, de 30 de noviembre de 2000, del Tribunal Constitucional (BOE núm. 4, 04-01-2001) (STC 292/2000).

A este respecto, cabe citar la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, 06-12-2018) (LOPDGDD), que tiene por objeto adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679.

Como consecuencia de lo anterior, la Dirección / Órgano de Gobierno de GENETRACER BIOTECH, S.L., ha asumido la máxima responsabilidad y compromiso con el establecimiento, implementación y mantenimiento de una Política de Protección de Datos en dicha entidad, garantizando la mejora continua con el objetivo de alcanzar la excelencia en relación con el cumplimiento del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018.

La Política de Protección de Datos de GENETRACER BIOTECH, S.L. descansa en el principio de «responsabilidad proactiva», según el cual el responsable del tratamiento es responsable del cumplimiento del marco normativo y jurisprudencial que gobierna dicha Política, y es capaz de demostrarlo ante las autoridades de control competentes.

No en vano, tal y como señala el considerando 74 del propio Reglamento (UE) 2016/679, los responsables del tratamiento están obligados a aplicar medidas oportunas y eficaces y han de poder demostrar la conformidad de las actividades de tratamiento con el referido Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas.

De acuerdo a lo señalado por el Grupo de Trabajo sobre protección de datos del artículo 29 (actual Comité Europeo de Protección de Datos), un «riesgo» es un escenario que describe un acontecimiento y sus consecuencias, estimado en términos de gravedad y probabilidad.

En tal sentido, la probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva

mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto (considerando 76).

Así mismo, como se indica en la declaración del citado Grupo de Trabajo sobre la función de un enfoque basado en el riesgo de los marcos jurídicos sobre protección de datos, la referencia a «los derechos y libertades» de las personas físicas atañe principalmente a los derechos a la protección de datos y a la intimidad, pero también puede implicar otros derechos fundamentales como la libertad de expresión, la libertad de pensamiento, la libertad de circulación, la prohibición de discriminación, el derecho a la libertad y la libertad de conciencia y de religión.

De tal modo, el considerando 75 del Reglamento general de protección de datos enumera una serie de factores o supuestos asociados a riesgos para los derechos y libertades de las personas físicas:

- Tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo;
- En los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales;
- En los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas;
- En los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales;
- En los casos en los que se traten datos personales de personas vulnerables, en particular niños; o
- En los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

De tal modo, la probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

A fin de mejorar el cumplimiento del Reglamento (UE) 2016/679, en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el citado Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento.

Como corolario de lo hasta aquí expuesto, el presente informe tiene como objeto dar cumplimiento con lo establecido en el artículo 35, apartado 1, del Reglamento (UE) 2016/679, según el cual «cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales».

Así mismo, el presente informe tiene como objeto dar cumplimiento con lo establecido en el artículo 28, apartado 1, de la Ley Orgánica 3/2018, según el cual:

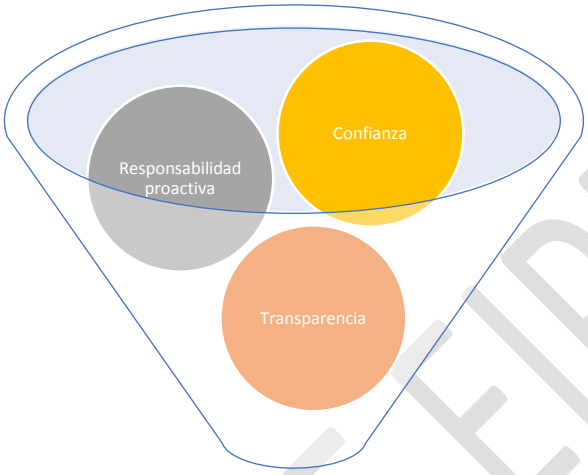
> *Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.*

En lo tocante a este particular, interesa subrayar que la publicación de la evaluación de impacto relativa a la protección de datos no representa un requisito jurídico del RGPD, ya que es una decisión que corresponde al responsable del tratamiento.

No obstante lo anterior, las Directrices del Grupo de Trabajo sobre protección de datos del artículo 29 (GT29) sobre la evaluación de impacto relativa a la protección de datos (EIPD),

subrayan expresamente que los responsables del tratamiento deben considerar al menos la publicación de alguna parte de su EIPD, como un resumen o una conclusión de la misma.

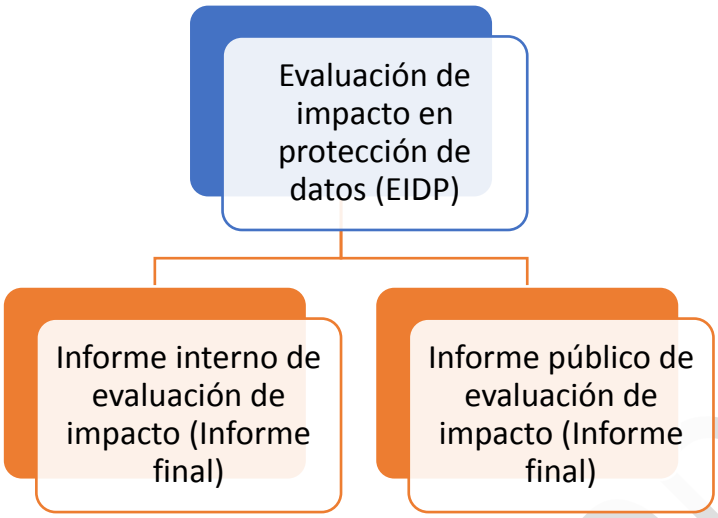
El fin de dicho proceso es ayudar a fomentar la confianza en las operaciones de tratamiento del responsable, y demostrar responsabilidad proactiva y transparencia. Cuando las personas se ven afectadas por la operación de tratamiento, la publicación de una EIPD supone una práctica particularmente positiva.



Publicación de la EIPD

Como consecuencia del compromiso de GENETRACER BIOTECH, S.L. con su propia Política de Protección de Datos, la citada entidad se rige, entre otros, por el principio de «licitud, lealtad y transparencia», según el cual los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado.

De tal modo, los resultados finales de la evaluación de impacto relativa a la protección de datos (EIPD) se dividen en un «Informe interno de evaluación de impacto» (Informe final), para su conocimiento por el Comité de Dirección u Órgano de Gobierno de la entidad responsable del tratamiento, y un «Informe público de evaluación de impacto» (Informe final), para fomentar la transparencia y la confianza de los interesados en las operaciones de tratamiento del responsable *(vid. gráfico página siguiente)*.



METODOLOGÍA EMPLEADA PARA LA REALIZACIÓN DE LA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (EIPD)

I. CONCEPTOS Y DEFINICIONES

A efectos del presente Informe se entenderá por:

a) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa 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 dicha persona.

b) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

c) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

d) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

e) «evaluación de impacto relativa a la protección de datos»: proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales, evaluándolos y determinando las medidas para abordarlos.

f) «habitual»: se asocia con uno o más de los siguientes significados:

- Continuado o que se produce a intervalos concretos durante un periodo concreto.
- Recurrente o repetido en momentos prefijados.
- Que tiene lugar de manera constante o periódica.

g) «sistemático»: se asocia con uno o más de los siguientes significados:

- Que se produce de acuerdo con un sistema.
- Preestablecido, organizado o metódico.
- Que tiene lugar como parte de un plan general de recogida de datos.

- Llevado a cabo como parte de una estrategia.

h) «a gran escala»: se tendrán en cuenta los siguientes factores a la hora de determinar si el tratamiento se realiza a gran escala:

- El número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente.
- El volumen de datos o la variedad de elementos de datos que son objeto de tratamiento.
- La duración, o permanencia, de la actividad de tratamiento de datos.
- El alcance geográfico de la actividad de tratamiento.

En particular, en relación con la evaluación de impacto relativa a la protección de datos se entenderá por:

a) «amenaza»: cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesados sobre cuyos datos personales se realiza un tratamiento.

b) «riesgo»: la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas.

c) «gestión de riesgos»: el conjunto de actividades y tareas que permiten controlar la incertidumbre relativa a una amenaza mediante una secuencia de actividades que incluyen la identificación y evaluación del riesgo, así como las medidas para su reducción o mitigación.

d) «riesgo inherente»: el riesgo intrínseco de cada actividad, sin tener en cuenta las medidas de control que mitigan o reducen su nivel de exposición.

e) «riesgo residual»: el riesgo que se obtiene una vez aplicadas las medidas de control para la reducción o mitigación del riesgo inherente.

f) «probabilidad»: posibilidades que existen de que la amenaza se materialice.

g) «impacto»: posibles daños que se pueden producir si la amenaza se materializa.

II. ¿QUÉ?, ¿CUÁL?, ¿CUÁNDO?, ¿QUIÉN?, ¿CÓMO?

A. ¿**QUÉ** ES UNA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (EIPD)?

El Reglamento (UE) 2016/679 establece la obligación para el responsable del tratamiento de aplicar «medidas técnicas y organizativas apropiadas», a fin de garantizar y poder demostrar que el tratamiento es conforme con el citado Reglamento, teniendo en cuenta «la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas» (art. 24.1 RGPD).

En su consecuencia, y atendiendo al principio de la «protección de datos desde el diseño», el responsable del tratamiento debe aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del Reglamento (UE) 2016/679 y proteger los derechos de los interesados. Para ello, deberá

tener en cuenta «el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas» (art. 25.1 RGPD).

Así mismo, dichas medidas deberán ser revisadas y actualizadas cuando sea necesario (art. 24.1 RGPD *in fine*).

En una misma línea, el artículo 35 del Reglamento (UE) 2016/679 establece, en su apartado primero, que cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento deberá realizar, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

En tal sentido, una EIPD o evaluación de impacto relativa a la protección de datos es, en esencia, un ejercicio de análisis de los riesgos que un determinado sistema de información, producto o servicio puede entrañar para el derecho fundamental a la protección de datos de los interesados y, tras ese análisis, afrontar la gestión eficaz de los riesgos identificados mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos.

No en vano, las propias Directrices sobre la evaluación de impacto relativa a la protección de datos, del Grupo de Trabajo sobre protección de datos del artículo 29, señalan que una EIPD es «un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales, evaluándolos y determinando las medidas para abordarlos».

De conformidad con lo establecido en el artículo 35, apartado 7, del RGPD, la evaluación deberá incluir como mínimo:

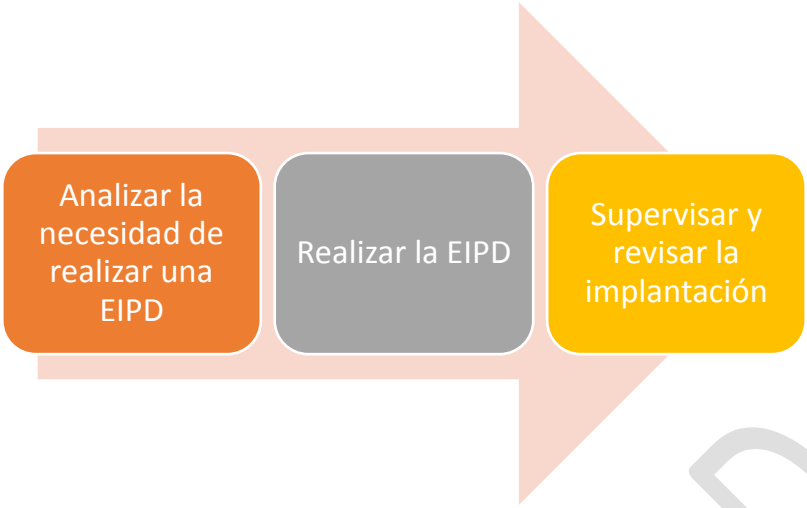
a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Siguiendo el esquema publicado por la Agencia Española de Protección de Datos en su «Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD», las diferentes fases de una evaluación de impacto relativa a la protección de datos y el flujo a seguir en la ejecución de la misma sería el siguiente *(vid. gráfico página siguiente)*:



En tal sentido, la estructura de la fase intermedia de realización de la evaluación de impacto relativa a la protección de datos contendría las siguientes etapas:

B. ¿**CUÁL** ES LA UTILIDAD DE UNA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (EIPD)?

Una EIPD o evaluación de impacto relativa a la protección de datos permite identificar los posibles riesgos y corregirlos anticipadamente, evitando los costes derivados de descubrirlos *a posteriori*, cuando el servicio está en funcionamiento o, lo que es peor, cuando la lesión de los derechos de los interesados ya se ha producido.

En tal sentido, la evaluación de impacto relativa a la protección de datos representa un instrumento práctico para ayudar a los responsables del tratamiento a cumplir la legislación de protección de datos.

Así mismo, según señalan las propias Directrices del GT29, las evaluaciones de impacto relativas a la protección de datos son instrumentos importantes para la rendición de cuentas, ya que ayudan a los responsables no solo a cumplir los requisitos del RGPD, sino también a demostrar que se han tomado medidas adecuadas para garantizar el cumplimiento del Reglamento (UE) 2016/679.

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

C. ¿**CUÁNDO** SE DEBE LLEVAR A CABO UNA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (EIPD)?

Siguiendo las Directrices del Grupo de Trabajo sobre protección de datos del artículo 29 (GT29), «en consonancia con el enfoque basado en el riesgo introducido por el RGPD, no resulta obligatorio realizar una EIPD en todas las operaciones de tratamiento». De tal modo, solo se exige la realización de una EIPD cuando sea probable que el tratamiento «entrañe un alto riesgo para los derechos y libertades de las personas físicas» (art. 35.1 RGPD).

En tal sentido, la obligación de los responsables del tratamiento de llevar a cabo una EIPD en determinadas circunstancias debe entenderse en el contexto de su obligación general de gestionar adecuadamente los riesgos derivados del tratamiento de datos personales.

Un «riesgo» es un escenario que describe un acontecimiento y sus consecuencias, estimado en términos de gravedad y probabilidad. Por otra parte, la «gestión de riesgos» puede definirse como las actividades coordinadas para dirigir y controlar una organización respecto al riesgo.

Como hemos señalado, el artículo 35 se refiere a un probable alto riesgo «para los derechos y libertades de las personas». Como se indica en la declaración del Grupo de Trabajo sobre

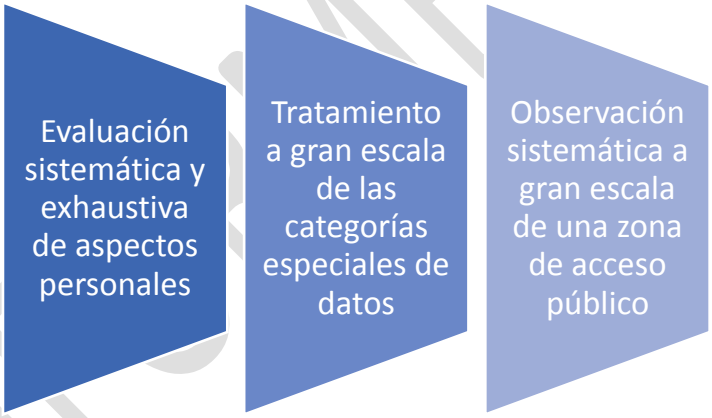
protección de datos del artículo 29 sobre la función de un enfoque basado en el riesgo de los marcos jurídicos sobre protección de datos, la referencia a «los derechos y libertades» de los interesados atañe principalmente a los derechos a la protección de datos y a la intimidad, pero también puede implicar otros derechos fundamentales como la libertad de expresión, la libertad de pensamiento, la libertad de circulación, la prohibición de discriminación, el derecho a la libertad y la libertad de conciencia y de religión.

Aunque en otras circunstancias pueda requerirse una EIPD, el artículo 35, apartado 3, ofrece algunos ejemplos de cuando una operación de tratamiento «es probable que entrañe un alto riesgo», señalando que la evaluación de impacto relativa a la protección de los datos se requerirá en particular en caso de:

a) *evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;*

b) *tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o*

c) *observación sistemática a gran escala de una zona de acceso público.*



A juicio del Grupo de Trabajo sobre protección de datos del artículo 29, las palabras «en particular» indicadas en la frase introductoria del artículo 35, apartado 3, del RGPD se refieren a una lista no exhaustiva. Pueden existir operaciones de tratamiento de «alto riesgo» que no estén incluidas en esta lista pero que supongan unos riesgos similarmente elevados. Estas operaciones de tratamiento también deben someterse a una EIPD. Por este motivo, los criterios desarrollados a continuación van, en ocasiones, más allá de una simple explicación de lo que debería entenderse a partir de los tres ejemplos indicados en el artículo 35, apartado 3, del RGPD.

En su consecuencia, los criterios que, a juicio del GT29, se deben considerar en relación con las operaciones de tratamiento que deben someterse a una evaluación de impacto relativa a la protección de datos, son los siguientes:

- Evaluación o puntuación, incluida la elaboración de perfiles y la predicción, especialmente de «aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud,

las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado» (considerandos 71 y 91 RGPD). Algunos ejemplos de esto podrán incluir a una institución financiera que investigue a sus clientes en una base de datos de referencia de crédito o en una base de datos contra el blanqueo de capitales y la financiación del terrorismo o sobre fraudes, o a una empresa de biotecnología que ofrezca pruebas genéticas directamente a los consumidores para evaluar y predecir los riesgos de enfermedad/salud, o a una empresa que elabore perfiles de comportamiento o de mercadotecnia basados en el uso o navegación en su sitio web.

- Toma de decisiones automatizada con efecto jurídico significativo o similar: tratamiento destinado a tomar decisiones sobre los interesados que produce «efectos jurídicos para las personas físicas» o que les afectan «significativamente de modo similar» (art. 35.3 a) RGPD). Por ejemplo, el tratamiento puede provocar exclusión o discriminación contra las personas. El tratamiento con poco o ningún efecto sobre las personas no coincide con este criterio específico.

- Observación sistemática: tratamiento usado para observar, supervisar y controlar a los interesados, incluidos los datos recogidos a través de redes u «observación sistemática (...) de una zona de acceso público» (art. 35.3 c) RGPD). Este tipo de observación representa un criterio porque los datos personales pueden ser recogidos en circunstancias en las que los interesados pueden no ser conscientes de quién está recopilando sus datos y cómo se usarán. Además, puede resultar imposible para las personas evitar ser objeto de este tipo de tratamiento en espacios públicos (o espacios de acceso público). El GT29 interpreta «zona de acceso público» como cualquier sitio abierto a cualquier persona, por ejemplo, una plaza, centro comercial, calle, mercado, estación de tren o biblioteca pública.

- Datos sensibles o datos muy personales: esto incluye las categorías especiales de datos personales definidas en el artículo 9 (por ejemplo, información sobre las opiniones políticas de las personas), así como datos personales relativos a condenas e infracciones penales según la definición del artículo 10. Un ejemplo sería un hospital general que guarda historiales médicos de pacientes o un investigador privado que guarda datos de delincuentes. Más allá de estas disposiciones del RGPD, puede considerarse que algunas categorías de datos aumentan el posible riesgo para los derechos y libertades de las personas. Estos datos personales se consideran sensibles (dado que este término es de uso común) porque están vinculados a hogares y actividades privadas (como comunicaciones electrónicas cuya confidencialidad debe ser protegida), porque afectan al ejercicio de un derecho fundamental (como datos de localización cuya recogida compromete la libertad de circulación) o porque su violación implica claramente graves repercusiones en la vida cotidiana del interesado (como datos financieros que podrían usarse para cometer fraude en los pagos). En este sentido, puede resultar relevante que los datos ya se hayan hecho públicos por el interesado o por terceras personas. El hecho de que los datos personales sean de acceso público puede considerarse un factor en la evaluación si estaba previsto que estos se usaran para ciertos fines. Este criterio también puede incluir datos tales como documentos personales, correos electrónicos, diarios, notas de lectores de libros electrónicos equipados con opciones para tomar notas e información muy personal incluida en aplicaciones de registro de actividades vitales.

- Tratamiento de datos a gran escala: el RGPD no define qué se entiende por gran escala, aunque el considerando 91 ofrece alguna orientación. En cualquier caso, el GT29

recomienda que se tengan en cuenta los siguientes factores, en particular, a la hora de determinar si el tratamiento se realiza a gran escala:

a. el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;

b. el volumen de datos o la variedad de elementos de datos distintos que se procesan;

c. la duración, o permanencia, de la actividad de tratamiento de datos;

d. el alcance geográfico de la actividad de tratamiento.

- Asociación o combinación de conjuntos de datos, por ejemplo, procedentes de dos o más operaciones de tratamiento de datos realizadas para distintos fines o por responsables del tratamiento distintos de una manera que exceda las expectativas razonables del interesado.

- Datos relativos a interesados vulnerables (considerando 75 RGPD): El tratamiento de este tipo de datos representa un criterio debido al aumento del desequilibrio de poder entre los interesados y el responsable del tratamiento, lo cual implica que las personas pueden ser incapaces de autorizar o denegar el tratamiento de sus datos, o de ejercer sus derechos. Entre los interesados vulnerables puede incluirse a niños (se considera que no son capaces de denegar o autorizar consciente y responsablemente el tratamiento de sus datos), empleados, segmentos más vulnerables de la población que necesitan una especial protección (personas con enfermedades mentales, solicitantes de asilo, personas mayores, pacientes, etc.), y cualquier caso en el que se pueda identificar un desequilibrio en la relación entre la posición del interesado y el responsable del tratamiento.

- Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas, como combinar el uso de huella dactilar y reconocimiento facial para mejorar el control físico de acceso, etc. El RGPD deja claro (art. 35.1 y considerandos 89 y 91 RGPD) que el uso de una nueva tecnología, definida «en función del nivel de conocimientos técnicos alcanzado» (considerando 91), puede hacer necesario realizar una EIPD. Esto es debido a que el uso de dicha tecnología puede implicar nuevas formas de recogida y utilización de datos, posiblemente con un alto riesgo para los derechos y libertades de las personas. De hecho, las consecuencias personales y sociales del despliegue de una nueva tecnología pueden ser desconocidas. Una EIPD ayudará al responsable del tratamiento a entender y abordar tales riesgos. Por ejemplo, algunas aplicaciones del «Internet de las cosas» podrían tener un impacto significativo sobre la vida diaria y la privacidad de las personas y, por tanto, requieren una EIPD.

- Cuando el propio tratamiento «impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato» (art. 22 y considerando 91 RGPD). Esto incluye operaciones de tratamiento destinadas a permitir, modificar o denegar el acceso de los interesados a un servicio o a un contrato. Un ejemplo de esto sería cuando un banco investiga a sus clientes en una base de datos de referencia de crédito con el fin de decidir si les ofrece un préstamo.

En la mayoría de los casos, un responsable del tratamiento puede considerar que un tratamiento que cumpla dos criterios requerirá la realización de una EIPD. En general, el GT29 considera que cuantos más criterios cumpla el tratamiento, más probable será que represente un alto riesgo para los derechos y libertades de los interesados y, por tanto, requiera una EIPD independientemente de las medidas que el responsable contemple adoptar. Sin embargo, en algunos casos, un responsable del tratamiento puede considerar que un tratamiento que cumpla solo uno de estos criterios requiere una EIPD.

En los casos en los que no esté claro si se requiere una evaluación de impacto relativa a la protección de datos, el GT29 recomienda realizar una, ya que, como hemos señalado con anterioridad, esta evaluación representa un instrumento práctico para ayudar a los responsables del tratamiento a cumplir la legislación de protección de datos.

Para facilitar a los responsables de los tratamientos la identificación de aquellos tratamientos que requieren una EIPD, el RGPD dispone que las autoridades de control deberán establecer y publicar una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos.

En este sentido, la Agencia Española de Protección de Datos ha publicado una «Lista orientativa de tipos de tratamiento que requieren una evaluación de impacto relativa a la protección de datos según artículo 35.4 RGPD».

En el momento de analizar tratamientos de datos será necesario realizar una EIPD en la mayoría de los casos en los que dicho tratamiento cumpla con dos o más criterios de la lista expuesta a continuación, salvo que el tratamiento se encuentre en la lista de tratamientos que no requieren EIPD a la que se refiere en artículo 35.5 del RGPD. Cuantos más criterios reúna el tratamiento en cuestión, mayor será el riesgo que entrañe dicho tratamiento y mayor será la certeza de la necesidad de realizar una EIPD.

Esta lista se basa en los criterios establecidas por el Grupo de Trabajo del Artículo 29 en la guía WP248 «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 RGPD», los complementa y debe entenderse como una lista no exhaustiva:

1. Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos.

2. Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.

3. Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.

4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.

5. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.

6. Tratamientos que impliquen el uso de datos genéticos para cualquier fin.

7. Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 «Directrices sobre los delegados de protección de datos (DPD)» del Grupo de Trabajo del Artículo 29.

8. Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos.

9. Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.

10. Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.

11. Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b, c, d) del RGPD.

D. ¿**QUIÉN** DEBE LLEVAR A CABO LA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (EIPD)?

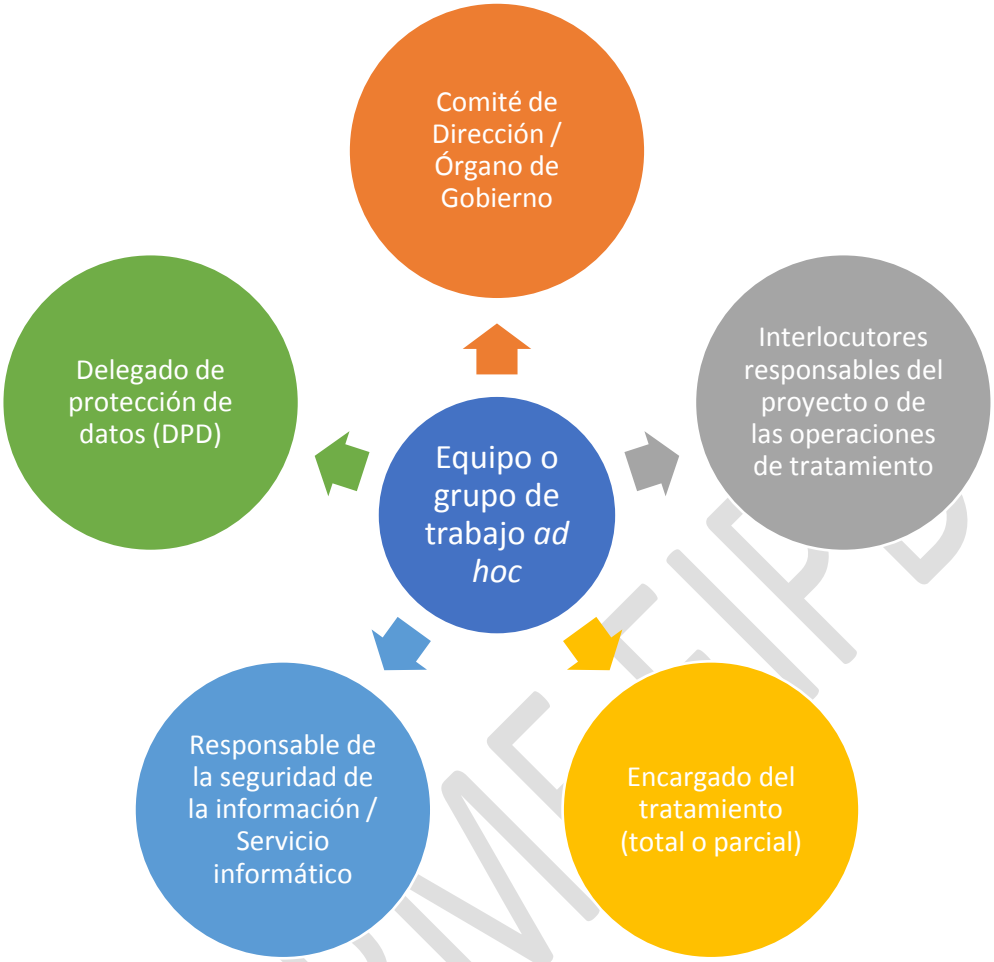
De conformidad con lo establecido en el artículo 35, apartado 1, del Reglamento (UE) 2016/679, y en el en el artículo 28, apartado 1, de la Ley Orgánica 3/2018, es el responsable del tratamiento quien debe garantizar que la evaluación de impacto relativa a la protección de datos se lleva a cabo. En tal sentido, cualquier otra persona, de dentro o fuera de la entidad, puede llevar a cabo una EIPD, pero el responsable del tratamiento sigue respondiendo en última instancia por la tarea realizada.

Señalado lo anterior, las Directrices del Grupo de Trabajo sobre protección de datos del artículo 29 (GT29) sobre la evaluación de impacto relativa a la protección de datos (EIPD), recomiendan «recabar el asesoramiento de expertos independientes (abogados, expertos en TI, expertos en seguridad, sociólogos, expertos en ética, etc.)» para la realización de la EIPD.

En su consecuencia, se ha constituido un grupo de trabajo multidisciplinar para la realización de la evaluación de impacto relativa a la protección de datos, bajo el asesoramiento de la Dirección Técnico-Jurídica de AUDIDAT.

Para llevar a cabo la EIPD, el citado equipo o grupo de trabajo necesita la imprescindible colaboración de otras partes intervinientes en el proceso de realización de la evaluación de impacto relativa a la protección de datos, cabiendo citar las siguientes:

- El Comité de Dirección u Órgano de Gobierno de la entidad responsable del tratamiento.
- Los interlocutores responsables del proyecto o de las operaciones de tratamiento objeto de la EIPD.
- El delegado de protección de datos (DPD) de la entidad responsable del tratamiento.
- El encargado que lleve a cabo el tratamiento total o parcialmente.
- El responsable de la seguridad de la información, en caso de ser nombrado, o el servicio informático de la entidad responsable del tratamiento.



En tal sentido, las funciones de cada una de las partes intervinientes en el proceso de realización de la evaluación de impacto relativa a la protección de datos serán las que a continuación se relacionan:

EQUIPO O GRUPO DE TRABAJO *AD HOC*
Bajo el asesoramiento de la Dirección Técnico-Jurídica de AUDIDAT, el equipo o grupo de trabajo multidisciplinar especialmente constituido a los efectos de la realización de la EIPD, debe encargarse de: a) obtener la información necesaria para el correcto desarrollo de la EIPD; b) asumir la interlocución con los otros sujetos intervinientes en el proceso de realización de la EIPD; c) planificar las tareas; d) organizar la realización de las consultas necesarias y evaluar los resultados; e) establecer las medidas que deben adoptarse para eliminar o mitigar los riesgos y recomendar su adopción; f) elaborar el «Informe interno de evaluación de impacto» (Informe final), para su conocimiento por el Comité de Dirección u Órgano de Gobierno de la entidad responsable del tratamiento; y g) elaborar el «Informe público de evaluación de impacto» (Informe final), para fomentar la transparencia y la confianza de los interesados en las operaciones de tratamiento del responsable.

COMITÉ DE DIRECCIÓN / ÓRGANO DE GOBIERNO
El Comité de Dirección u Órgano de Gobierno de la entidad responsable del tratamiento es el encargado de aprobar las políticas y procedimientos. También debe aprobar las desviaciones y excepciones a la práctica normal. En su consecuencia, es fundamental contar con la participación del mismo para establecer y apoyar la función de gestión de riesgos propia de la EIPD.

INTERLOCUTORES RESPONSABLES DEL PROYECTO O DE LAS OPERACIONES DE TRATAMIENTO
Una EIPD puede afectar a una única operación de tratamiento de datos. Sin embargo, el artículo 35.1 del RGPD establece que *"una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares"*. En tal sentido, los responsables del proyecto o de las operaciones de tratamiento deben permanecer a disposición del equipo o grupo de trabajo multidisciplinar especialmente constituido a los efectos de la realización de la EIPD, a fin de que éste pueda obtener la información necesaria para el correcto desarrollo de la EIPD.

DELEGADO DE PROTECCIÓN DE DATOS (DPD)
El artículo 35.2 del RGPD establece específicamente que el responsable del tratamiento *"recabará el asesoramiento"* del DPD cuando realice una evaluación de impacto relativa a la protección de datos. A su vez, el artículo 39.1 c) del RGPD, impone al DPD la obligación de *"ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35"*. El GT29 recomienda que el responsable del tratamiento busque el asesoramiento del DPD en las siguientes cuestiones, entre otras: a) si debe llevarse a cabo o no una evaluación de impacto relativa a la protección de datos; b) qué metodología debe seguirse al llevar a cabo una evaluación de impacto; c) si debe realizarse la evaluación de impacto en la propia organización o subcontratarse; d) qué salvaguardias (incluidas medidas técnicas y organizativas) deben aplicarse para mitigar cualquier riesgo para los derechos e intereses de los interesados; e) si la evaluación de impacto relativa a la protección de datos se ha llevado a cabo correctamente o no y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardias aplicar) son conformes con el RGPD.

ENCARGADO DEL TRATAMIENTO (TOTAL O PARCIAL)
El GT29 ha señalado que, si un encargado lleva a cabo el tratamiento total o parcialmente, dicho encargado debe ayudar al responsable a realizar la EIPD y debe ofrecer la información necesaria, de acuerdo al artículo 28.3 f) del RGPD. En tal sentido, si un encargado lleva a cabo el tratamiento total o parcialmente, debe permanecer a disposición del equipo o grupo de trabajo multidisciplinar especialmente constituido a los efectos de la realización de la EIPD, a fin de que éste pueda obtener la información necesaria para el correcto desarrollo de la EIPD.

RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN / SERVICIO INFORMÁTICO
El GT29 ha señalado que el responsable de la seguridad de la información, en caso de ser nombrado, o el servicio informático de la entidad responsable del tratamiento, debería ayudar en las siguientes cuestiones: a) qué metodología debe seguirse al llevar a cabo una evaluación de impacto; b) evaluar la calidad de la evaluación del riesgo y si el riesgo residual es aceptable; c) desarrollar conocimientos específicos para el contexto del responsable del tratamiento (necesidades de seguridad y operativas).

Siguiendo las recomendaciones de la Agencia Española de Protección de Datos en su "Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD", la asignación de responsabilidades de cada una de las partes intervinientes en el proceso de realización de la evaluación de impacto relativa a la protección de datos, puede realizarse en base a las siguientes figuras de responsabilidad recogidas en la metodología RACI:

- **RESPONSIBLE (R):** responsable de realizar la tarea.
- **ACCOUNTABLE (A):** responsable de que la tarea se realice, sin necesidad de ser el que la ejecute y responsable de rendir cuentas sobre su ejecución.
- **CONSULTED (C):** figura que debe ser consultada para la realización de la tarea.
- **INFORMED (I):** figura que debe ser informada sobre la realización de la tarea.

En su consecuencia, las responsabilidades asignadas a cada una de las partes intervinientes en el proceso de realización de la evaluación de impacto relativa a la protección de datos son las que a continuación se relacionan:

PARTE INTERVINIENTE EN EL PROCESO	RESPONSABILIDAD ASIGNADA
Equipo o grupo de trabajo *ad hoc*	• Responsible (R)
Comité de Dirección / Órgano de Gobierno	• Accountable (A) • Informed (I)
Interlocutores responsables del proyecto o de las operaciones de tratamiento	• Consulted (C)
Delegado de protección de datos (DPD)	• Consulted (C) • Informed (I)
Encargado del tratamiento (total o parcial)	• Consulted (C)
Responsable de la seguridad de la información / Servicio informático	• Consulted (C)

E. ¿**CÓMO** SE DEBE REALIZAR UNA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (EIPD)?

De conformidad con lo señalado por la Agencia Española de Protección de Datos en su «Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD», es fundamental disponer de un proceso sistemático a través de una metodología o procedimiento estandarizado de trabajo que permita establecer criterios comunes para garantizar la homogeneidad, repetitividad y comparabilidad en la ejecución de una EIPD.

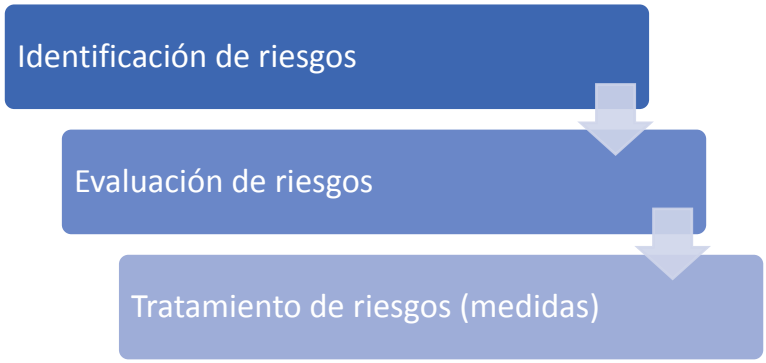
Siguiendo el esquema publicado por la Agencia Española de Protección de Datos, la metodología empleada para la evaluación de impacto relativa a la protección de datos incluye las siguientes fases:

1. Análisis preliminar	•**Analizar la necesidad** de realizar una EIPD
2. Contexto	•**Describir el ciclo de vida** de los datos •**Analizar la necesidad y proporcionalidad** del tratamiento
3. Gestión de riesgos	•**Identificar** amenazas y riesgos •**Evaluar** los riesgos •**Tratar** los riesgos
4. Conclusión y validación	•**Plan de acción** •Informe de **conclusiones**
5. Consulta (en caso de alto riesgo residual)	•**Consultar** a la autoridad de control el riesgo residual aceptable •**Informe favorable** de la autoridad
6. Supervisión	•**Supervisión** de la implantación •**Revisión** post-implantación •**Fin** de la EIPD

De todas las fases relacionadas, la parte troncal y, por ende, más importante de la evaluación de impacto relativa a la protección de datos es la relativa a la «gestión de riesgos».

Según la Agencia Española de Protección de Datos, la «gestión de riesgos» es el conjunto de actividades y tareas que permiten controlar la incertidumbre relativa a una amenaza mediante una secuencia de actividades que incluyen la identificación y evaluación del riesgo, así como las medidas para su reducción o mitigación.

En tal sentido, la «gestión de riesgos» se divide, básicamente, en las tres fases siguientes: identificación de riesgos, evaluación de riesgos y tratamiento de riesgos.



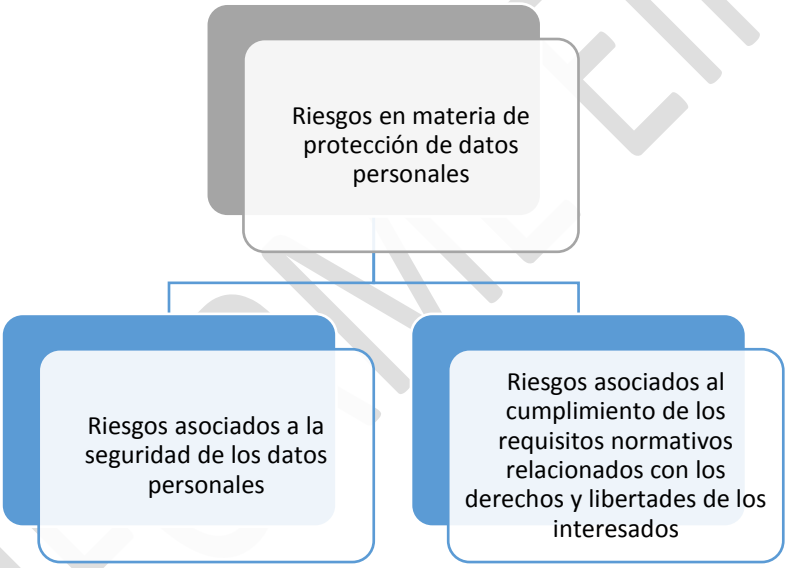
FASE 1: IDENTIFICACIÓN DE RIESGOS

Para la Agencia Española de Protección de Datos, un «riesgo» se puede definir como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas.

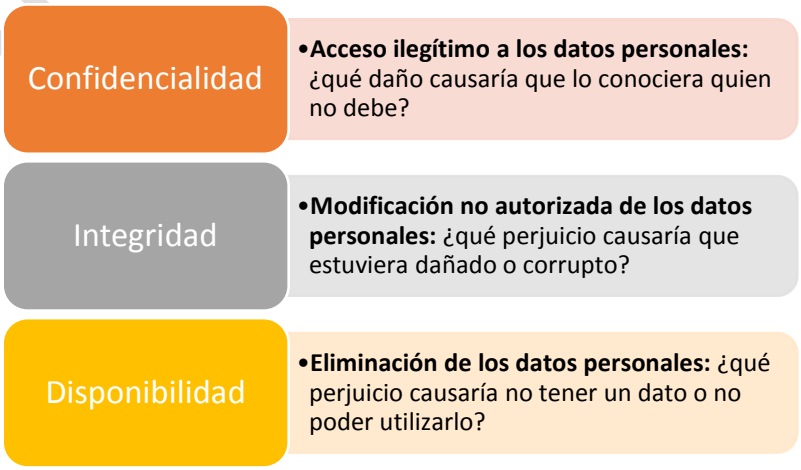
Así mismo, una «amenaza» es cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesados sobre cuyos datos personales se realiza un tratamiento.

Como puede observarse, las amenazas y los riesgos asociados están directamente relacionados. En su consecuencia, la identificación de los riesgos comporta, en todo caso, considerar las amenazas que los pueden originar.

Desde la óptica de la protección de datos personales, los principales riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, se pueden categorizar en dos dimensiones básicas: a) riesgos asociados a la seguridad de los datos personales y b) riesgos asociados al cumplimiento de los requisitos normativos relacionados con los derechos y libertades de los interesados.



a) **Riesgos asociados a la seguridad de los datos personales**, desde su triple vertiente: Confidencialidad, Integridad y Disponibilidad (CIA) de los datos personales.



b) Riesgos asociados al cumplimiento de los requisitos normativos relacionados con los derechos y libertades de los interesados, y en particular los relacionados con la garantía del cumplimiento de los principios relativos al tratamiento de los datos personales (por ejemplo, el uso ilícito de datos personales) y del ejercicio de los derechos de los interesados (por ejemplo, no tener implementado un protocolo para la atención al ejercicio de derechos).

Garantía de los principios relativos al tratamiento de los datos personales

- Licitud, lealtad y transparencia.
- Limitación de la finalidad.
- Minimización de datos.
- Exactitud.
- Limitación del plazo de conservación.
- Integridad y confidencialidad.

Garantía del ejercicio de los derechos de los interesados

- Deben existir modelos a disposición de los interesados para el ejercicio de cada uno de sus derechos.
- Las solicitudes deben responderse en el plazo máximo de un mes.
- Cuando la solicitud se presente por medios electrónicos, la información debe facilitarse por medios electrónicos.
- Cuando la solicitud no sea estimada, debe informarse del derecho a presentar una reclamación ante la autoridad de protección de datos.

FASE 2: EVALUACIÓN DE RIESGOS

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

El cálculo del riesgo inherente se realiza mediante la siguiente fórmula:

Riesgo = Probabilidad X Impacto

La «probabilidad» se determina en base a las posibilidades que existen de que la amenaza se materialice. En tal sentido, se utilizará una metodología de evaluación de la probabilidad basada en cuatro niveles posibles (despreciable / limitada / significativa / máxima), de acuerdo con lo recogido en la norma ISO/IEC 29134:2017 “Directrices para la evaluación de impacto sobre la privacidad”:

ESCALA DE PROBABILIDAD	
PROBABILIDAD DESPRECIABLE	La probabilidad de ocurrencia es **muy baja** (por ejemplo, un evento que puede pasar de forma fortuita).
PROBABILIDAD LIMITADA	La probabilidad de ocurrencia es **baja** (por ejemplo, un evento que puede pasar de forma ocasional).
PROBABILIDAD SIGNIFICATIVA	La probabilidad de ocurrencia es **alta** (por ejemplo, un evento que puede pasar con bastante frecuencia).
PROBABILIDAD MÁXIMA	La probabilidad de ocurrencia es **muy elevada** (por ejemplo, un evento cuya ocurrencia se produce con mucha frecuencia).

El «impacto» se determina en base a los posibles daños que se pueden producir si la amenaza se materializa. De igual modo, se utilizará una metodología de evaluación del impacto basada en cuatro niveles posibles (despreciable / limitado / significativo / máximo), de acuerdo con lo recogido en la norma ISO/IEC 29134:2017 "Directrices para la evaluación de impacto sobre la privacidad":

ESCALA DE IMPACTO	
IMPACTO DESPRECIABLE	El impacto es **muy bajo** (por ejemplo, un evento cuyas consecuencias son prácticamente despreciables sin impacto sobre el interesado).
IMPACTO LIMITADO	El impacto es **bajo** (por ejemplo, un evento cuyas consecuencias implican un daño menor sin impacto relevante sobre el interesado).
IMPACTO SIGNIFICATIVO	El impacto es **alto** (por ejemplo, un evento cuyas consecuencias implican un daño elevado con impacto relevante sobre el interesado).
IMPACTO MÁXIMO	El impacto es **muy alto** (por ejemplo, un evento cuyas consecuencias implican un daño muy elevado con impacto crítico sobre el interesado).

Tomando como base las escalas de probabilidad e impacto, para poder determinar el riesgo inherente, es necesario asignar valores numéricos a cada uno de los niveles de las escalas de probabilidad e impacto. La escala de asignación de valores numéricos comprende desde el valor 1, en el caso de que la magnitud sea despreciable, hasta el valor 4 en el caso donde la magnitud es máxima:

ESCALA DE VALORES	
1	Despreciable
2	Limitado
3	Significativo
4	Máximo

Enfrentando las escalas de valores de probabilidad e impacto se obtiene la «matriz de riesgos», en base a la fórmula «Riesgo = Probabilidad X impacto»:

PROBABILIDAD	Máxima 4	**4**	**8**	**12**	**16**
	Significativa 3	**3**	**6**	**9**	**12**
	Limitada 2	**2**	**4**	**6**	**8**
	Despreciable 1	**1**	**2**	**3**	**4**
MATRIZ DE RIESGOS		Despreciable 1	Limitado 2	Significativo 3	Máximo 4
		IMPACTO			

Determinando, en función de la escala de asignación de valores numéricos predefinida, el valor de la probabilidad y el valor del impacto, se obtiene una posición en la matriz de riesgos que se corresponde con el riesgo inherente, resultado de aplicar la fórmula «Riesgo = Probabilidad X impacto».

En función del valor obtenido como resultado de la aplicación de la fórmula para el cálculo del riesgo inherente, se determina el nivel de riesgo inherente (bajo / medio / alto / muy alto), en base a la siguiente escala:

NIVEL DE RIESGO INHERENTE	
BAJO	Si el valor resultante se sitúa entre los valores 1 y 2.
MEDIO	Si el valor resultante es mayor de 2 y menor o igual que 6.
ALTO	Si el valor resultante es mayor que 6 y menor o igual que 9.
MUY ALTO	Si el valor resultante es mayor que 9.

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

FASE 3: TRATAMIENTO DE RIESGOS

En esta fase de la gestión de riesgos se deben definir las medidas necesarias para disminuir la probabilidad y/o el impacto de que se materialice una amenaza en materia de protección de datos personales.

Dependiendo de la estrategia utilizada en cada caso concreto, las medidas de control propuestas pueden clasificarse en los siguientes tipos:

Tipología de medidas de control	
Medidas dirigidas a mitigar el riesgo inherente	Desarrollo de acciones concretas que, o bien disminuyan la probabilidad de que se materialice la amenaza, o bien disminuyan su impacto en caso de que se acabe materializando (por ejemplo, realizar copias periódicas de seguridad de los datos personales).
Medidas dirigidas a eliminar el riesgo inherente	Establecimiento de medidas que modifiquen por completo las condiciones originales a partir de las cuales se genera la amenaza (por ejemplo, retirar una cámara de videovigilancia).
Medidas dirigidas a aceptar el riesgo inherente	Aceptación del riesgo inherente, estableciendo, de forma paralela, un protocolo de actuación que se active en el caso de que la amenaza se acabe materializando.
Medidas dirigidas a transferir el riesgo inherente	Traslado del impacto negativo del riesgo hacia un tercero (por ejemplo, contratar un seguro o introducir una cláusula específica de responsabilidad en el contrato con un proveedor).

Debe tenerse en cuenta que el riesgo cero no existe, por lo que, independientemente de su tipología, el conjunto de las medidas de control tiene como objetivo final minimizar el riesgo hasta un nivel aceptable, que permita al responsable del tratamiento garantizar los derechos y libertades de los interesados, a la vez que continúa ejerciendo su actividad propia en iguales o similares condiciones. Es lo que se conoce como «riesgo residual aceptable».

CONSULTA PREVIA

En virtud de lo dispuesto en el art. 35.1 Reglamento (UE) 2016/679, "*El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo*".

En caso de implantarse y aplicarse de manera efectiva las medidas mitigadoras del riesgo propuestas, se obtiene como resultado la eliminación de aquellos tratamientos de datos que conllevan un alto riesgo dentro de la entidad, por lo que no sería necesario realizar una consulta previa a la Agencia Española de Protección de Datos y el tratamiento podría continuar de manera conforme con el Reglamento (UE) 2016/679.

RESUMEN EJECUTIVO DE LA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

La Evaluación de Impacto en la Protección de Datos Personales es una herramienta que ha permitido al responsable del tratamiento evaluar los potenciales riesgos a los que están expuestos los datos personales que se encuentran bajo su responsabilidad, teniendo en cuenta para ello las actividades de tratamiento que se desarrollan con los mismos.

En primer lugar, se ha analizado el ciclo de vida de la información y el flujo de datos propios del tratamiento, actividad esencial en este tipo de estudios desde el momento en que permite conocer el proceso al que se somete la información tratada. Así, se han identificado los datos objeto de tratamiento, los intervinientes del proceso y a terceras entidades y sistemas implicados, registrando así cualquier elemento relevante que participe en la actividad de tratamiento.

No obstante, y teniendo en cuenta que este análisis no debe considerarse como una actividad aislada, es fundamental señalar que debe existir un fluido canal de comunicación entre las áreas involucradas en las operaciones del tratamiento, de manera tal que pueda obtenerse información relevante sobre el ciclo de vida de los datos asociados al tratamiento de manera continua y el responsable del tratamiento siempre se encuentre en disposición de definirlo.

La necesidad y proporcionalidad del tratamiento de datos también han sido objeto de análisis en la presente evaluación de impacto relativa a la protección de datos. El responsable del tratamiento ha sido capaz de demostrar que es necesario proceder con el tratamiento de datos objeto de análisis, respetando para ello todos los principios relativos al tratamiento recogidos en el art. 6 Reglamento (UE) 2016/679.

Una vez el responsable ha determinado la necesidad y proporcionalidad del tratamiento y ha analizado el ciclo de vida del dato y establecido los focos de riesgo, éstos se han clasificado atendiendo a las posibilidades reales de que la amenaza se materialice y al impacto que tendría cada actividad sobre los derechos y libertades de los interesados. La identificación y evaluación de los distintos otorga al responsable del tratamiento una posición que le permite tratarlos, proponiendo para ello una serie de medidas de control que reducirán el riesgo inherente de las operaciones de tratamiento.

De esta manera, el responsable del tratamiento cuenta con un plan de acción que le permitirá demostrar, desde el momento en que aplique las medidas de manera efectiva, que se garantizan los derechos y libertades de las personas y la seguridad de los datos en el normal desarrollo de su actividad propia.

Sin embargo, esta evaluación de impacto relativa a la protección de datos no es sino un ejercicio teórico que requiere su puesta en práctica de forma íntegra para garantizar los derechos y las libertades de los interesados. Es fundamental que se realice una adecuada supervisión y una posterior revisión de la implantación de las medidas de control definidas en la EIPD para reducir el riesgo inherente hasta un riesgo residual que permita llevar a cabo el tratamiento garantizando los derechos y libertades de las personas físicas.

Debe tenerse en cuenta que el riesgo cero no existe, por lo que las medidas de control propuestas tienen como objetivo minimizar el riesgo asociado a una operación de tratamiento hasta un nivel aceptable para poder llevar a cabo las mismas garantizando los derechos y libertades de los interesados.

Por todo ello:

La evaluación de impacto relativa a la protección de datos realizada por la persona jurídica GENETRACER BIOTECH S.L. ha tenido un resultado:

FAVORABLE

La actividad de tratamiento se podrá llevar a cabo **siempre y cuando se implanten las medidas de control incluidas en el plan de acción recogido en el presente «Informe interno de evaluación de impacto en la protección de datos (Informe final)»**, pues de esa manera no existirá un alto riesgo para los derechos y libertades de los interesados en relación con las operaciones de tratamiento analizadas

Como corolario a todo lo hasta aquí expuesto, debe subrayarse que la evaluación de impacto es un proceso continuo que no se agota con la emisión del presente informe, ya que, como bien determina el Reglamento (UE) 2016/679, deberá revisarse si los tratamientos siguen siendo conformes con la evaluación a la que hubieran sido sometidos y, en todo caso, hacerlo cuando exista un cambio sustancial en alguna de las operaciones de tratamiento.