GUÍA

para una Evaluación de Impacto en la Protección de Datos Personales

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

GUÍA
para una Evaluación de Impacto en la Protección de Datos Personales

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

índice

1. INTRODUCCIÓN

La Agencia Española de Protección de Datos (AEPD) apuesta por trabajar en nuevos enfoques y nuevas herramientas que permitan hacer frente con mayor eficacia a la profunda transformación que se está produciendo en el ámbito del tratamiento de la información personal como consecuencia de la continua irrupción de nuevas tecnologías en un entorno social fuertemente marcado por la globalización.

En este contexto, cada día se ponen en circulación nuevos productos y servicios que hacen un uso intensivo de los datos personales y tienen un fuerte impacto en la esfera de la vida privada.

En consecuencia, la información personal adquiere cada vez un mayor valor económico y, por ello, resulta imprescindible complementar los planteamientos tradicionales con nuevos enfoques proactivos que contribuyan a respetar los derechos de las personas y a fortalecer la confianza de los clientes y usuarios.

Ello no implica en modo alguno que se haya de abandonar el enfoque basado en la exigencia de cumplimiento de las disposiciones legales, sino que para garantizar este cumplimiento se hace cada vez más necesaria una disposición diligente, un compromiso responsable para evitar o minimizar los riesgos antes de que estos se materialicen.

En la línea de fortalecer la responsabilidad proactiva de quienes tratan datos personales en los sectores público y privado resultan especialmente útiles enfoques como el de la Privacidad desde el Diseño, que propugna que las cuestiones de protección de datos y privacidad se tomen en consideración desde la fase inicial, desde el momento mismo del diseño de un producto o servicio.

Con ello se consigue no solo una mayor eficacia en la protección de los derechos de los afectados, sino también evitar algo que sucede con demasiada frecuencia: la reconvención a posteriori de la

norma a la tecnología de tal forma que, una vez que ésta ha sido desarrollada o implantada, se aprecia su ilegalidad y ello lleva consigo altos costes para su rediseño y adaptación.

Y entre las herramientas más útiles para avanzar en la privacidad desde el diseño se encuentran las Evaluaciones de Impacto en la Privacidad o en la Protección de Datos, más conocidas como PIAs, por sus siglas en inglés (Privacy Impact Assessments), que se han desarrollado fundamentalmente en países anglosajones, donde ya existen metodologías consolidadas para su realización.

Una PIA o una Evaluación de Impacto en la Protección de los Datos Personales (EIPD) 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 afectados y, tras ese análisis, afrontar la gestión eficaz de los riesgos identificados mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos.

La gran ventaja derivada de la realización de una EIPD en las etapas iniciales del diseño de un nuevo producto, servicio o sistema de información es que 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 se ha producido. En estos casos no solo se incurre en costes económicos, sino también de imagen para la organización cuya reputación se ve afectada.

Además, la realización de una EIPD es un excelente ejercicio de transparencia, base de una relación de confianza. Ayuda a planificar las respuestas a posibles impactos en la protección de datos de los afectados, a gestionar las relaciones con terceras partes implicadas en el proyecto y a educar y motivar a los empleados para estar alerta sobre posibles problemas o incidentes en relación con el tratamiento de datos personales.

En España no existe en estos momentos una obligación legal de realizar Evaluaciones de Impacto de esta naturaleza en ningún sector o ámbito específico, aunque podría existir en el futuro si se aprueba la Propuesta de Reglamento General de Protección de Datos para la Unión Europea en los términos propuestos por la Comisión Europea.

Pero, en todo caso, con independencia de que exista o no una exigencia normativa, la AEPD considera que se trata de una metodología que ha alcanzado ya un grado de desarrollo suficiente como para considerarla madura y plenamente incorporable a nuestro país.

Su empleo mejorará sin duda las garantías para los derechos de las personas en aquellas organizaciones que las incorporen a sus sistemas y procedimientos de gestión de la privacidad, y contribuirá a generar más confianza en los usuarios y clientes de las mismas.

La Agencia ha decidido elaborar esta *Guía para la Evaluación de Impacto en la Protección de los Datos Personales* con el objeto de promover una cultura proactiva de la privacidad, proporcionando un marco de referencia para el ejercicio de ese compromiso responsable que, a la vez, contribuya a fortalecer la protección eficaz de los derechos de las personas.

Además, en su desarrollo se ha querido contar con la opinión de la sociedad y, por ello, se redactó un primer borrador que fue sometido a consulta pública durante seis semanas. En las respuestas a dicha consulta se constató una valoración muy positiva de la Guía. Un porcentaje superior al 90% de quienes respondieron consideraron su estructura adecuada, un 82% entendió que el lenguaje y los términos en los que estaba redactada eran correctos y un 86% manifestó que los criterios incluidos para decidir sobre la necesidad de realizar una EIPD eran apropiados. Asimismo, los comentarios y sugerencias recibidas han aportado valiosas reflexiones que se han tenido en cuenta para la redacción de la versión final de este documento.

Y aunque, como luego se abordará, la realización de una Evaluación de Impacto en la Protección de Datos (EIPD) va más allá de la verificación del cumplimiento normativo, ello no impide que las EIPD se constituyan también en un elemento eficaz y destacado de los sistemas, procedimientos y métodos de la organización para asegurar el cumplimiento de la normativa de protección de datos.

Esta Guía no pretende ser la única manera en que puede llevarse a efecto una EIPD. Las organizaciones que tengan ya implantados procesos y herramientas de análisis de riesgos podrían utilizarlas para evaluar los relativos a la privacidad y la protección de datos siempre que cubran los aspectos esenciales que toda Evaluación de Impacto en la Protección de Datos debe tener y que se detallan, a modo de contenido mínimo, en la siguiente sección de este documento.

Por lo tanto, la Guía está concebida como un marco flexible, que proporciona un modelo estructurado en el que apoyarse pero que no es invariable. Mientras se respeten sus aspectos fundamentales, cada organización podrá (e incluso deberá) adaptarlo a su estructura, a su cultura y a sus necesidades.

Además, la Agencia siempre dará la bienvenida a iniciativas sectoriales que, manteniendo los elementos esenciales contenidos en esta Guía, propongan las modulaciones o especificaciones que sean convenientes para su adaptación a las necesidades concretas de cada sector.

Adicionalmente, la realización de una Evaluación de Impacto siguiendo las directrices de la Guía, aunque no podrá ser considerada como un criterio de exención de eventuales responsabilidades en caso de que se incurra en una vulneración de la normativa de protección de datos, sí será teni-

da en cuenta por la Agencia como un elemento relevante a la hora de valorar si se ha adoptado la diligencia debida en la implementación de las medidas adecuadas para cumplir con las exigencias legales.

La Agencia Española de Protección de Datos desea que todos aquellos a quienes va dirigido este documento –organizaciones y profesionales– lo encuentren adecuado, atractivo e interesante, y que les resulte un instrumento útil para integrar esta herramienta de las EIPD en el ejercicio de sus funciones durante la concepción, diseño, desarrollo y puesta en marcha de nuevos productos, servicios y sistemas de información.

2. CONCEPTO

Una Evaluación de Impacto en la Protección de Datos Personales (EIPD) es un análisis de los riesgos que un producto o servicio puede entrañar para la protección de datos de los afectados y, como consecuencia de ese análisis, la gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos.

Una EIPD es una herramienta que va más allá de una evaluación de cumplimiento normativo –aunque, obviamente, la verificación de dicho cumplimiento es una parte integral de cualquier EIPD– y que se adentra tanto en las expectativas de privacidad que tienen las personas ante cualquier tratamiento de sus datos personales como en las percepciones generales de la sociedad o, concretamente, de los colectivos más afectados por el tratamiento del que se trate.

Existen muchas definiciones de Evaluación de Impacto en la Protección de Datos[1]. Una de las más conocidas y que se propuso en un primer momento es la que las considera como «un proceso donde se lleva a cabo un esfuerzo consciente y sistemático para evaluar el impacto en la protección de datos personales de las opciones que pueden adoptarse en relación con una determinada propuesta o proyecto» o como «una evaluación de cualesquiera efectos actuales o potenciales que una determinada propuesta o proyecto podrían tener en la privacidad individual y las formas en las que estos efectos adversos se pueden mitigar»[2].

Otra más reciente es la que caracteriza una EIPD como «una metodología para evaluar el impacto en la privacidad de un proyecto, política, programa, servicio, producto o cualquier iniciativa que implique el tratamiento de datos personales y, tras haber consultado con todas

[1] En realidad, de *Privacy Impact Assessments* como son conocidas en los países de lengua inglesa donde nacieron. Aunque los conceptos no son absolutamente coincidentes, son de utilidad para el objetivo de esta Guía.

[2] Stewart, B. Privacy impact assessments. Privacy Law and Policy Reporter. Australia (1996). El autor ha reconocido que provienen de una adaptación de las utilizadas para los análisis de impacto medioambiental, dado que existen paralelismos entre ambos procesos.

las partes implicadas, tomar las medidas necesarias para evitar o minimizar los impactos negativos. Una evaluación de impacto en la privacidad es un proceso que debería comenzar en las etapas más iniciales que sea posible, cuando todavía hay oportunidades de influir en el resultado del proyecto»[3].

En cualquier caso, a través de la evolución de los trabajos e investigaciones, se ha constatado que hay un conjunto de elementos comunes que forman parte del núcleo de cualquier procedimiento que se pueda considerar como una evaluación de impacto en el derecho fundamental a la protección de datos personales:

- Una EIPD es un proceso más amplio que el de la mera comprobación del cumplimiento normativo, que debe llevarse a cabo con anterioridad a la implantación de un nuevo producto, servicio o sistema de información o cuando uno existente vaya a sufrir cambios sustanciales que impliquen la posibilidad de la aparición de nuevos riesgos.
- Debe ser sistemática y reproducible, y estar orientada a revisar procesos más que a producir un resultado o informe final. Además, debe permitir una identificación clara de los responsables de las distintas tareas.
- Comienza con una primera fase de identificación y clasificación de la información para determinar los datos personales que se tratan y sus características.
- Debe identificar quién y cómo tendrá acceso y tratará los datos personales.
- Se debe permitir participar en el proceso y realizar aportaciones a todos los afectados por el mismo, tanto departamentos de la organización como socios o entidades externas, afectados u otros agentes sociales.
- Debe contener una descripción de los controles que se implantarán para asegurar que solo se tratan los datos personales necesarios y para las finalidades legítimas previstas y definidas.
- El resultado final debe ser un documento con un contenido mínimo y una estructura que deben definirse previamente.

[3] Wright, D., De Hert, P. Privacy Impact Assessment. Springer (2012).

– Este resultado final de una EIPD debería tener un cierto grado de publicidad en un documento distribuido por la organización que la ha realizado y que, por supuesto, no contendrá información confidencial o sensible.

La gran ventaja derivada de la realización de una evaluación de impacto en el momento oportuno, esto es, en las etapas iniciales del diseño de un nuevo producto, servicio o sistema de información, es la identificación de los posibles riesgos que pueden derivarse del mismo y su corrección –o, al menos, su mitigación- antes de que el sistema se desarrolle y se descubran a posteriori, implicando generalmente una solución con elevados costes.

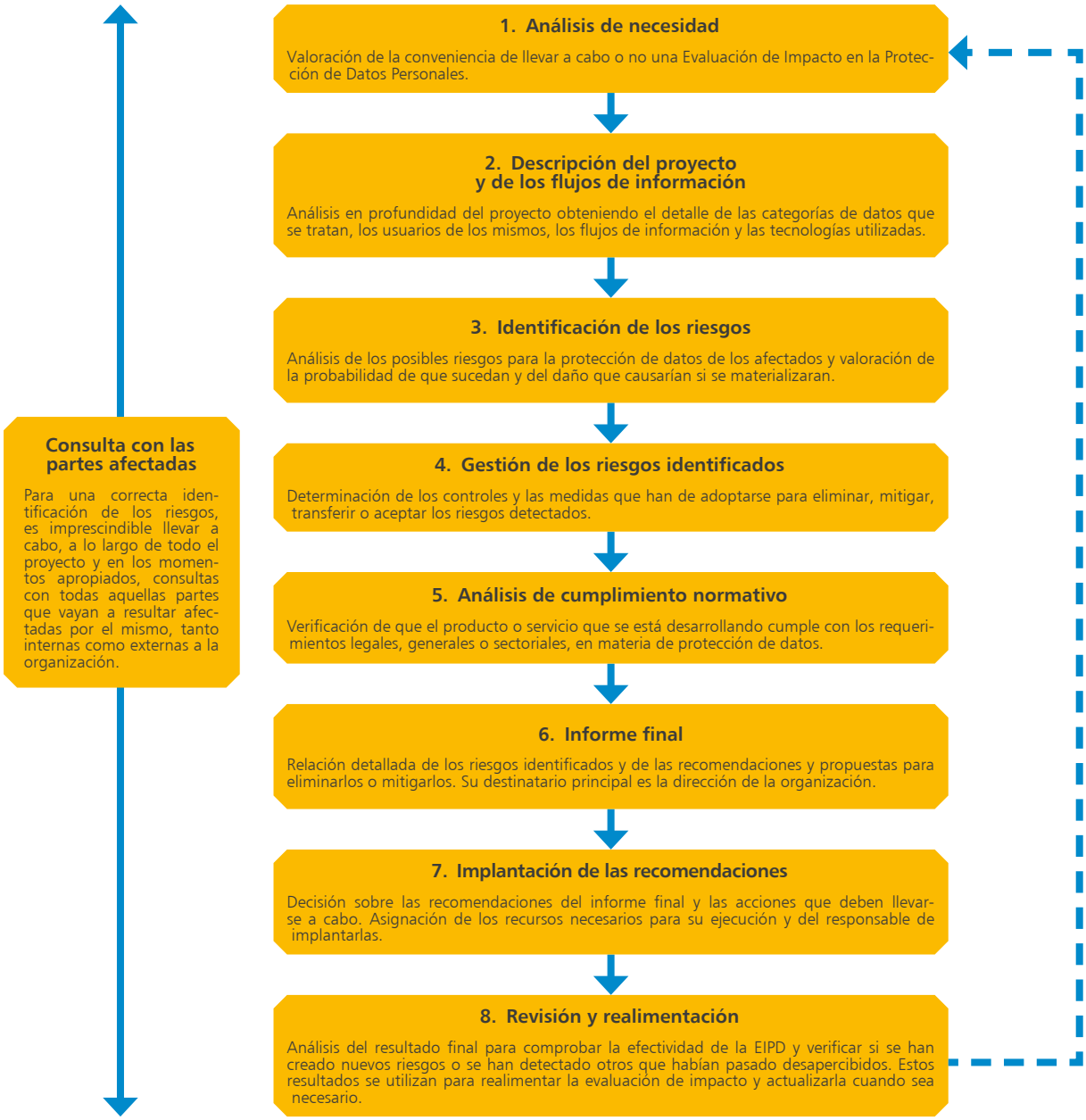
Además, no solo hay que tener en cuenta los costes económicos sino también las posibles consecuencias negativas para la imagen y la reputación de la organización y la gran frustración que se genera entre todos los implicados en el proyecto por la necesidad de rehacer un trabajo ya finalizado y reabrir cuestiones de diseño e implantación que ya se habían resuelto.

Una vez que el proyecto ha finalizado, se deberían llevar a cabo revisiones periódicas para verificar si los riesgos previstos han desaparecido o se han mitigado de la forma esperada y para comprobar si han aparecido otros nuevos que requieran una actuación complementaria. Los resultados de estas revisiones son nuevos elementos que habrán de tenerse en cuenta para decidir si es necesario revisar la EIPD y, en su caso, establecer nuevas medidas[4].

A continuación, para facilitar una visión general de las fases de las que se compone una EIPD y antes de pasar a una descripción detallada de las mismas, se incluye un esquema de los pasos esenciales de los que consta.

[4] Estas revisiones no deben confundirse con las auditorías que prescribe el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD).

FASES PRINCIPALES DE UNA EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS



3. ANÁLISIS DE LA NECESIDAD DE LA EVALUACIÓN

Antes de adentrarse en los aspectos concretos de realización de una EIPD es fundamental llevar a cabo una reflexión previa sobre las situaciones que aconsejarían su realización, ya que pequeños cambios o proyectos que no signifiquen modificaciones importantes o nuevos usos de datos personales pueden no justificar, por su sencillez y escasos riesgos para la privacidad, la realización de una evaluación de impacto.

Por otra parte, no todas las EIPD tienen por qué realizarse con la misma intensidad ni con el mismo grado de profundidad. Habrá casos en los que será posible llevarlas a cabo de una manera menos exhaustiva y formalizada (porque se ponga de manifiesto que los riesgos son escasos o fácilmente mitigables) mientras que en otras situaciones podrían incluso requerirse acciones adicionales a las aquí recogidas por la complejidad o la importancia de los riesgos existentes.

Además, hay que hacer hincapié en que, independientemente de las características del proyecto de que se trate, el tipo, actividad y tamaño de la organización juegan un papel importante a la hora de decidir sobre la necesidad de realizar una EIPD como la que propone este documento.

En efecto, en pequeñas o medianas organizaciones o en aquellas cuya actividad no implique un tratamiento masivo de datos de carácter personal o no esté orientada a la explotación de los mismos con finalidades que supongan una invasión notable de la privacidad[5], sería posible decidirse por una aproximación menos formalizada que, teniendo en cuenta los principios básicos que a continuación se van a exponer, conlleve una reflexión seria y responsable sobre los tratamientos de datos personales que se vayan a llevar a efecto y, así, detectar y minimizar los riesgos para los derechos de los afectados que los mismos pudieran entrañar.

[5] Como, por ejemplo, la monitorización del comportamiento o la publicidad basada en el mismo, la elaboración de perfiles de cualquier tipo, la verificación de la idoneidad para determinadas tareas, la evaluación de la personalidad o de la situación financiera, laboral, social, familiar, formación, gustos o aficiones y las que impliquen el tratamiento de datos especialmente protegidos.

En relación con las situaciones en las que sería aconsejable llevar a cabo una evaluación de impacto, a continuación se incluye una relación indicativa de algunas de ellas:

- Cuando se enriquezca la información existente sobre las personas mediante la recogida de nuevas categorías de datos o se usen las existentes con nuevas finalidades o en formas que antes no se usaban, en particular, si los nuevos usos o finalidades son más intrusivos o inesperados para los afectados.
- Cuando se lleve a cabo un tratamiento significativo no incidental de datos de menores o dirigido especialmente a tratar datos de estos, en particular si tienen menos de catorce años.
- Cuando se vaya a llevar a cabo un tratamiento destinado a evaluar o predecir aspectos personales relevantes de los afectados[6], su comportamiento, su encuadramiento en perfiles determinados (para cualquier finalidad)[7], encaminado a tomar medidas que produzcan efectos jurídicos que los atañen o los afectan significativamente y, en particular, cuando establezcan diferencias de trato o trato discriminatorio[8] o que puedan afectar a su dignidad o su integridad personal[9].
- Cuando se traten grandes volúmenes de datos personales a través de tecnologías como la de datos masivos (*Big data*), internet de las cosas (*Internet of Things*) o el desarrollo y la construcción de ciudades inteligentes (*smart cities*).
- Cuando se vayan a utilizar tecnologías que se consideran especialmente invasivas con la privacidad como la videovigilancia a gran escala, la utilización de aeronaves no tripuladas (*drones*), la vigilancia electrónica, la minería de datos, la biometría, las técnicas genéticas, la geolocalización, o la utilización de etiquetas de radiofrecuencia o RFID[10] (especialmente,

---

[6] Como, por ejemplo, su estado de salud, fiabilidad o adecuación para tareas determinadas, situación financiera, laboral, social (en particular, en relación con la concesión de beneficios o subsidios), familiar (estructura familiar, datos de menores…), su ideología, creencias, formación, gustos, aficiones, compras, etc.

[7] Como, por ejemplo, para servirles publicidad personalizada.

[8] Especialmente cuando se vayan a tomar decisiones que afectan de manera significativa a determinados colectivos o individuos, que establezcan diferencias entre ellos o puedan comportar un riesgo de discriminación de cualquier tipo (económica, social, política, racial, sexual, etc.) como, por ejemplo, la concesión o denegación de un determinado beneficio social, el ajuste de tarifas o precios o la oferta diferenciada de productos o servicios en función de los datos personales que se traten.

[9] Por ejemplo, a través de la monitorización y el análisis de la conducta de las personas (historiales de navegación y actividades en internet, comunicaciones, movimientos, historiales de lectura, compras, transacciones electrónicas, participación en foros, redes sociales, blogs o cualquier otra actividad en línea).

[10] Ver el documento «Privacy and Data Protection Impact Assessment Framework for RFID Applications. Bruselas (2011)» y el Dictamen 9/2011 relativo a la Propuesta Revisada de la Industria para un Marco de Evaluación del Impacto sobre la Protección de Datos y la Intimidad en las Aplicaciones Basadas en la Identificación por Radiofrecuencia (RFID) del Grupo de Trabajo del Artículo 29.

si forman parte de la llamada internet de las cosas) o cualesquiera otras que puedan desarrollarse en el futuro.

- Cuando el tratamiento afecte a un número elevado de personas o, alternativa o adicionalmente, se produzca la acumulación de gran cantidad de datos respecto de los interesados.
- Cuando se cedan o comuniquen los datos personales a terceros y, en particular, siempre que se pongan en marcha nuevas iniciativas que supongan compartir datos personales con terceros que antes no tenían acceso a ellos, ya sea entregándolos, recibiéndolos o poniéndolos en común de cualquier forma.
- Cuando se vayan a transferir los datos a países que no forman parte del Espacio Económico Europeo (EEE)[11] y que no hayan sido objeto de una declaración de adecuación por parte de la Comisión Europea o de la Agencia Española de Protección de Datos[12].
- Cuando se vayan a utilizar formas de contactar con las personas afectadas que se podrían considerar especialmente intrusivas.
- Cuando se vayan a utilizar datos personales no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica.
- Cuando la recogida tenga como finalidad el tratamiento sistemático y masivo de datos especialmente protegidos.

Si el proyecto se incardina en cualquiera de las categorías detalladas y, especialmente, si está en varias de ellas, teniendo en cuenta las salvedades realizadas al comienzo de esta sección, se debería considerar la realización de una EIPD.

Un elemento adicional que debería tenerse en cuenta para decidir si los riesgos para la privacidad se incrementan de manera que harían aconsejable la realización de una EIPD, aunque no estuviéramos en presencia de alguna de las anteriores circunstancias, es la existencia de riesgos específicos de seguridad que puedan comprometer la confidencialidad, la integridad o la disponibilidad de los datos personales y, especialmente, si estas situaciones de riesgo se producen cuando los datos circulan o se accede a ellos a través de redes de telecomunicaciones.

---

[11] Los Estados miembros de la UE además de Islandia, Liechtenstein y Noruega. Las transferencias a terceros países declarados adecuados por la Comisión Europea o la Agencia Española de Protección de Datos, aun implicando riesgos menores, suponen, en cualquier caso, el que los datos personales se traten en una jurisdicción con un sistema de garantías menor que el de los Estados miembros del EEE.

[12] En *Decisiones de Adecuación de la Comisión Europea* se pueden consultar la lista de las mismas.

En cualquier caso, aunque el proyecto no se ajuste a los tratamientos que se acaban de detallar y, por lo tanto, no parezca un candidato a ser sometido a una EIPD, hay que resaltar que todo proyecto para el establecimiento de un nuevo sistema de información, producto o servicio -o su actualización- se beneficia en gran medida si los aspectos de protección de datos se toman en cuenta y se analizan antes del inicio de los trabajos, aunque sea de una manera más informal y no tan detallada como el proceso que se describe en este documento y, al menos, se lleva a cabo un análisis de cumplimiento normativo de las regulaciones de protección de datos que le sean de aplicación.

De cualquier forma, hay que poner de manifiesto que siempre es una buena práctica que una organización decida llevar a cabo una evaluación de impacto en relación con tratamientos que no están entre los mencionados y asegurarse de que no le van a pasar desapercibidos posibles riesgos que, de no atajarlos, podrían tener consecuencias legales, económicas o reputacionales.

La realización de las EIPD puede integrarse dentro de las metodologías de análisis de riesgos y las listas de actividades de las herramientas de gestión de proyectos existentes en las organizaciones. El único requisito es que se tengan en cuenta los elementos esenciales de las EIPD y que se asegure que se ha realizado una revisión cuidadosa y sistemática del nuevo proyecto para identificar todos los posibles riesgos para la privacidad y un esfuerzo serio por eliminarlos o reducirlos a un nivel aceptable y razonable.

Antes de finalizar este apartado resulta necesario realizar un apunte en relación con procesos de disociación o anonimización de datos personales que implicarían la no aplicabilidad de la legislación de protección de datos personales y, por ende, la irrelevancia de la realización de una EIPD[13].

La utilización de pseudónimos es una medida adecuada de salvaguarda de la privacidad e incluso sirve para mitigar los riesgos para la misma. No obstante, hay que señalar que la utilización de esta técnica no convierte los datos personales en anónimos pues, por definición, un pseudónimo es siempre reversible y, por lo tanto, es posible averiguar quién es la persona que está detrás del mismo[14].

---

[13] Ver el «Dictamen 05/2014, sobre técnicas de anonimización» aprobado por el Grupo de Trabajo de Protección de Datos (Grupo del Artículo 29) el 10 de abril de 2014 en el sitio web de la Comisión Europea (ec.europa.eu).

[14] Además, la elección poco cuidadosa de pseudónimos o su generación sistemática podría ofrecer directamente posibilidades para la identificación de las personas a las que se les atribuyen.

Del mismo modo, hay que resaltar que los datos pseudonimizados también pueden ser objeto de tratamiento y utilizarse para tomar decisiones sobre las personas (incluso de gran trascendencia y que les afectan directamente), aunque no se sepa su identidad nominativa.

Asimismo, la utilización de técnicas de compresión de la información, cifrado, segmentación de la misma en distintas bases de datos o utilización de códigos para conectar datos en posesión de distintos responsables y evitar que alguno de ellos acceda directamente a la identidad de los afectados[15] no implica en modo alguno que los datos a los que se les aplican dejen de ser datos personales. Por lo tanto, si los tratamientos que se van a realizar con ellos se encuentran en el catálogo antes expuesto, dichos tratamientos serían candidatos a ser sometidos a una EIPD y, por supuesto, estarían sujetos a la legislación de protección de datos.

Una vez revisados los elementos principales que deberían tenerse en cuenta para decidir sobre la realización de una EIPD y sus conceptos clave, se va a proceder al establecimiento de las fases que se deberían abordar para la sistematización y estructuración del proceso.

[15] Técnica muy habitual, por ejemplo, en tratamientos de datos personales ligados a ensayos clínicos.

4. CONSTITUCIÓN DEL EQUIPO DE TRABAJO Y DEFINICIÓN DE SUS TÉRMINOS DE REFERENCIA

Antes de comenzar propiamente las tareas para llevar a cabo una EIPD es conveniente reflexionar sobre quiénes deben ser los encargados de realizarla y los resultados esperados de su trabajo.

El fruto de esta reflexión debe ser la creación de un equipo o grupo de trabajo interdisciplinar que se encargue de obtener la información necesaria para un correcto desarrollo de la EIPD, asuma la interlocución con los responsables del proyecto y con la dirección de la organización, planifique las tareas, realice las consultas necesarias, evalúe los resultados, establezca las medidas que deben adoptarse para eliminar o mitigar los riesgos, recomiende su adopción y elabore el informe final.

Pero antes de entrar en los detalles de las personas que deberían formar parte de este equipo de trabajo, hay que hacer hincapié en que dicho equipo, para que pueda tener éxito en su labor, debe contar con el apoyo y el compromiso de la alta dirección de la organización, ya que sin ellos es muy difícil que sus tareas se puedan desarrollar adecuadamente.

No existen reglas fijas sobre quién debería participar en el grupo o liderarlo, pues dependerá mucho de la organización de que se trate, su tamaño, estructura y cultura particular, así como del proyecto que se vaya a evaluar.

En cualquier caso, sí se pueden ofrecer unas directrices sobre quiénes no podrían faltar en el mismo: un representante –con capacidad de decisión– del proyecto sometido a evaluación, el delegado de protección de datos o la persona que ejerza esta responsabilidad (o el asesor externo al que se le haya confiado esta misión), el responsable de seguridad y representantes cualificados del departamento TIC y de las áreas de negocio o departamentos a los que más afecte el proyecto dentro de la organización.

El siguiente aspecto que habría que determinar es el alcance de la EIPD, esto es, sus términos de referencia, que deben incluir una definición clara del proyecto que se va a evaluar, el contenido y

extensión de la evaluación, el tiempo previsto, la forma en que se presentarán las conclusiones y recomendaciones, los mecanismos de implantación y revisión de las medidas recomendadas y la estructura del informe final que se elaborará como resultado de la evaluación.

Es aconsejable que tanto la composición del equipo, su dirección y las atribuciones de sus miembros como los términos de referencia de la EIPD se plasmen en un documento formal aprobado por el grupo de trabajo y por la dirección.

Asimismo, y aunque será posible su adaptación o modificación basándose en los resultados parciales y provisionales y en la experiencia del equipo, hay que definir el contenido general y los apartados básicos del documento que se presentará y se publicará (en todo o en parte) como resultado del proceso de evaluación. Como ya se ha mencionado, una EIPD debe estar orientada a procesos y no a producir un informe formal, pero no por ello debe descuidarse el contenido mínimo y la manera en que se presentarán los resultados del mismo, ya que será un elemento fundamental para informar a la dirección y a todos los actores implicados.

Este hecho debe tenerse en cuenta para redactar este informe en un lenguaje claro y comprensible que huya de tecnicismos tanto legales como tecnológicos y que exprese claramente el objetivo del proyecto, los flujos de información, los riesgos identificados, las consultas realizadas y las soluciones propuestas o implantadas. En la sección correspondiente de esta Guía se realiza una sugerencia sobre su contenido mínimo y en el Anexo III se incluye un posible modelo.

5. DESCRIPCIÓN DEL PROYECTO Y DE LOS FLUJOS DE DATOS PERSONALES

El detalle con el que se pueda llevar a cabo este paso depende en gran manera del momento en que se realice la EIPD. En efecto, si la misma tiene lugar en la fase inicial del proyecto (estudio de viabilidad, establecimiento de objetivos y requerimientos generales, definición genérica de funcionalidades, etc.) la información con la que se cuente será todavía limitada y, por ello, es posible que también lo sea el resultado de este paso.

Si este fuera el caso, habría que volver a repasar y a actualizar esta fase una vez lo permita el propio avance y desarrollo del proyecto y se disponga de información adicional más detallada.

En cualquier caso, una correcta cumplimentación de este paso es crucial para realizar una evaluación de impacto adecuada y significativa y para la identificación de los riesgos para la privacidad. El contenido de esta documentación pondrá de manifiesto los objetivos, los actores implicados, las categorías de datos que se tratarán, las tecnologías utilizadas, las comunicaciones a terceros, la necesidad de utilizar o no todos los datos previstos, la necesidad que tienen los participantes de acceder y utilizar datos personales o categorías de datos personales específicas, etc.

De hecho, si una organización no conoce y comprende completamente los flujos de los datos personales que utiliza y cómo se usan, este hecho sería, en sí mismo, un grave riesgo para la privacidad que debería eliminarse mediante las tareas de documentación apropiadas.

La claridad con la que se expongan todos estos apartados es fundamental y para ello, además de utilizar un lenguaje claro, directo y comprensible, es de máxima importancia la inclusión de material gráfico que explique, de forma visual y resumida, las principales características del proyecto y de los flujos de información.

Algunos apartados básicos que deberían abordarse y documentarse en esta fase son los siguientes:

- Un resumen del proyecto con sus principales características, incluyendo una descripción de su necesidad u oportunidad para la organización.
- Identificación de aquellos aspectos del proyecto especialmente relevantes para la privacidad de las personas y que sean susceptibles de generar más riesgos[16] o de dificultar el cumplimiento normativo.
- Una descripción detallada de:
  a. Los medios de tratamiento y de las tecnologías que se utilizarán y, en particular, de aquellas que introduzcan mayores riesgos para la privacidad.
  b. Las categorías de datos personales que se van a tratar, finalidades para las que se usarán cada una de ellas, necesidad de su utilización y colectivos afectados.
  c. Quién accederá a cada categoría de datos personales y los motivos y justificaciones para ello.
  d. Los flujos de información: recogida, circulación dentro de la organización, cesiones fuera de la misma y recepciones de datos personales procedentes de otras organizaciones[17].
- Si resulta necesario, incluir información y diagramas adicionales para ilustrar aspectos como el control de acceso o la conservación o destrucción de los datos personales.

En este paso, los datos procedentes de estudios o auditorías anteriores o de inventarios de activos pueden resultar relevantes y muy útiles para ayudar en la confección de documentación adecuada.

Como ya se ha mencionado, en el caso de que no se pueda proporcionar toda la información descrita por el hecho de que aún no se dispone de ella en el momento en que se inicia la evaluación, se debería incluir la que estuviera disponible en ese momento y volver de nuevo a revisar este apartado en una fase más avanzada del diseño, estimando cómo impacta la nueva información en las conclusiones o decisiones alcanzadas inicialmente.

En el Anexo II de esta Guía se incluye un posible modelo para sistematizar, resumir y gestionar esta fase de la EIPD que puede ser utilizado por aquellas organizaciones que así lo deseen.

---

[16] Por ejemplo, la generación de perfiles, tratamiento de datos especialmente protegidos, toma de decisiones o acciones con impacto relevante en los afectados o tratamientos especialmente intrusivos para la privacidad.

[17] La inclusión de diagramas, gráficos y otros elementos visuales resulta de ayuda para esta finalidad. Para su confección se pueden utilizar los que se produzcan a través de las metodologías y herramientas de gestión de proyectos que utilice la organización.

6. IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS PARA LA PROTECCIÓN DE DATOS

En este momento comienza específicamente la evaluación de impacto que el proyecto tendrá en la protección de datos personales, a través del análisis de toda la documentación generada y, en particular, del seguimiento del ciclo de vida de los datos personales, sus usos previstos, las finalidades para las que se tratarán, las tecnologías utilizadas y la identificación de los usuarios que accederán a ella para, así, conocer los riesgos, reales y percibidos, existentes para la privacidad.

Los riesgos pueden ser de dos tipos. El primero y principal es el que afecta a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos.

Pero tampoco hay que descuidar los riesgos que puede afrontar una organización por no haber implantado una correcta política de protección de datos o por haberlo hecho de forma descuidada o errática, sin poner en marcha mecanismos de planificación, implantación, verificación y corrección eficaces.

Entre estos riesgos podemos incluir los derivados de una percepción de falta de respeto a la privacidad o de cumplimiento de las expectativas de privacidad de las personas, lo que puede motivar una baja utilización de los productos o servicios ofertados; la aparición o el incremento de los costes de rediseño del sistema e, incluso, la retirada del mismo; la falta de apoyo de actores clave para la viabilidad del proyecto; la pérdida de reputación e imagen pública y, por supuesto, la posibilidad de acciones de investigación y, en su caso, sancionadoras por parte de la autoridad de protección de datos competente.

Antes de pasar a la identificación de los posibles riesgos para la privacidad que podemos encontrar al realizar una EIPD es conveniente formalizar la noción de riesgo: un riesgo es la probabilidad de

que una amenaza se materialice aprovechando una vulnerabilidad de los sistemas de información o, dicho de otra manera, la probabilidad de que ocurra un incidente que cause un impacto con un determinado daño en los sistemas de información.

Por lo tanto, a pesar de las limitaciones y dificultades que pueda tener el expresar en el lenguaje natural acciones relativas a amenazas, vulnerabilidades y probabilidades que inciden en los riesgos para el derecho fundamental a la protección de datos personales, las descripciones que se realizan a continuación deben entenderse desde esta perspectiva: la probabilidad de que suceda un hecho que produzca un daño a la privacidad de las personas cuyos datos se tratan o a la reputación de la organización que realiza esta actividad.

A continuación se detallan una serie de riesgos cuya presencia debería ser comprobada en el nuevo sistema de información, producto o servicio y, en caso de detectarlos, se deberían adoptar las medidas necesarias para eliminarlos o, si ello no es posible, al menos mitigarlos o minimizarlos[18].

RIESGOS

Generales

- Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales
- Pérdidas económicas y daños reputacionales derivados del incumplimiento de legislaciones sectoriales con incidencia en la protección de datos personales a las que pueda estar sujeto el responsable del tratamiento

[18] Ello no quiere decir que no existan otros riesgos que no se han identificado en este catálogo y que pudieran aparecer al analizar cualesquiera nuevos productos, servicios o sistemas de información, sobre todo teniendo en cuenta los nuevos desarrollos tecnológicos que se producen continuamente.

Además, es necesario señalar que no es ni puede ser el objetivo de esta Guía el proporcionar criterios ni metodologías para definir cuantitativamente los niveles de riesgo de cada una de las situaciones descritas y de cualesquiera otras que pudieran aparecer como fuentes de riesgo para la privacidad al realizar una EIPD. Estas valoraciones han de ser llevadas a cabo en función del producto o servicio de que se trate, de las circunstancias de tratamiento de los datos, de los destinatarios de los mismos, de las tecnologías utilizadas, etc.

En este sentido, los modelos incluidos en los anexos son sencillas tablas sin más pretensión que servir de ayuda y orientación a aquellas organizaciones que no cuentan con experiencia previa en este ámbito de la gestión de riesgos. La AEPD es consciente de que existen múltiples metodologías y productos comerciales mucho más elaborados que proporcionan niveles de detalle y sofisticación mucho mayores.

- Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de las mismas, en particular, cuando se producen pérdidas de datos personales
- Pérdida de competitividad del producto o servicio derivada de los daños reputacionales causados por una deficiente gestión de la privacidad
- Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados
- Incorporación tardía de los expertos en protección de datos (en particular, del delegado de protección de datos o DPO) al proyecto o definición deficiente de sus funciones y competencias

Legitimación de los tratamientos y cesiones de datos personales

- Tratar o ceder datos personales cuando no es necesario para la finalidad perseguida
- Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales
- Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales
- Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión
- Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros
- Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardias necesarias
- Enriquecer los datos personales de forma no prevista en las finalidades iniciales y sin la información adecuada a los afectados al realizar una interconexión con otras bases de datos de la organización o de terceros, en particular, la re-identificación de información disociada
- Utilizar cookies de seguimiento u otros mecanismos de rastreo sin obtener un consentimiento válido tras una información adecuada[19]
- Impedir la utilización anónima de un determinado producto o servicio cuando la identificación del usuario no resulta indispensable

Transferencias internacionales

- Acceso secreto a los datos personales por parte de autoridades de terceros países
- Carencia de mecanismos de control de cumplimiento de las garantías establecidas para la transferencia
- Impedimentos por parte del importador para el ejercicio de los procedimientos de supervisión y control pactados
- Incapacidad de ayudar a los ciudadanos en el ejercicio de sus derechos ante el importador
- No obtención de las autorizaciones legales necesarias

[19] Ver *Guía sobre el uso de las cookies* de la Agencia Española de Protección de Datos redactada en colaboración con Adigital, Autocontrol e IAB. Canal de Publicaciones en www.agpd.es

Notificación de los tratamientos

- Carecer de los mecanismos y procedimientos necesarios para detectar cuándo debe notificarse la creación, modificación o cancelación de un tratamiento de datos personales a la AEPD o a la autoridad de protección de datos competente

Transparencia de los tratamientos

- Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada (cookies, ubicación geográfica, comportamiento, hábitos de navegación, etc.)
- En el entorno web, ubicar la información en materia de protección de datos (políticas de privacidad, cláusulas informativas) en lugares de difícil localización o diseminada en diversas secciones y apartados que dificulten su acceso conjunto y detallado
- Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida que los afectados se hagan una idea clara y ajustada de los elementos esenciales que deben conocer para que exista un tratamiento leal de sus datos personales

Calidad de los datos

- Solicitar datos o categorías de datos innecesarios para las finalidades del nuevo sistema, producto o servicio
- Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados con informaciones diferentes o contradictorias, lo que puede derivar en la toma de decisiones erróneas
- Garantías insuficientes para el uso de datos personales con fines históricos, científicos o estadísticos
- Utilizar los datos personales para finalidades no especificadas o incompatibles con las declaradas
  - Datos transaccionales, de navegación o de geolocalización para la monitorización del comportamiento, la realización de perfiles y la toma de decisiones sobre las personas.
  - Toma de decisiones económicas, sociales, laborales, etc. relevantes sobre las personas (en particular las que pertenecen a colectivos vulnerables[20]), especialmente si pueden ser adversas o discriminatorias, incluyendo diferencias en los precios y costes de servicios y productos o trabas para el paso de fronteras.
  - Toma de decisiones automatizadas con posibles consecuencias relevantes para las personas.
  - Utilización de los metadatos para finalidades no declaradas o incompatibles con las declaradas.
- Realizar inferencias o deducciones erróneas (y, en su caso, perjudiciales) sobre personas específicas mediante la utilización de técnicas de inteligencia artificial (en particular, minería de datos), reconocimiento facial o análisis biométricos de cualquier tipo
- Carecer de procedimientos claros y de herramientas adecuadas para garantizar la cancelación de oficio de los datos personales una vez que han dejado de ser necesarios para la finalidad o finalidades para las que se recogieron

[20] Testigos protegidos, víctimas de violencia de género, menores, personas amenazadas, con nuevas identidades, desempleadas, dependientes, desfavorecidas o receptoras de asistencia social o sociosanitaria, discapacitadas, enfermas mentales o con enfermedades que generan rechazo social, etc.

Datos especialmente protegidos

- Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso cuando este sea la causa que legitima su tratamiento o cesión
- Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos sensibles
- Disociación deficiente o reversible que permita la re-identificación de datos sensibles en procesos de investigación que solo prevén utilizar datos anónimos

Deber de secreto

- Accesos no autorizados a datos personales
- Violaciones de la confidencialidad de los datos personales por parte de los empleados de la organización

Tratamientos por encargo

- Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas
- Falta de diligencia (o dificultad para demostrarla) en la elección del encargado de tratamiento
- Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad
- No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos ARCO realizados ante los encargados de tratamiento
- Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato

Derechos ARCO

- Dificultar o imposibilitar el ejercicio de los derechos ARCO
- Carencia de procedimientos y herramientas para la gestión de los derechos ARCO
- Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales

Seguridad

- Inexistencia de Responsable de Seguridad o deficiente definición de sus funciones y competencias
- Inexistencia de política de seguridad
- Deficiencias organizativas en la gestión del control de accesos
- Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales
- Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información
- Uso de identificadores que revelan información del afectado
- Deficiencias en la protección de la confidencialidad de la información
- Falta de formación del personal sobre las medidas de seguridad que están obligados a adoptar y sobre las consecuencias que se pueden derivar de no hacerlo
- Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc.) para terceros no autorizados

En este punto hay que señalar que no basta con la identificación de los riesgos para la protección de datos personales sino que es imprescindible realizar una cuantificación de los mismos en dos aspectos: probabilidad de que sucedan y nivel de impacto en la privacidad que tendría su materialización.

Esta cuantificación es completamente dependiente del proyecto y de las circunstancias y el entorno en que se va a producir el despliegue del nuevo producto o servicio y el tratamiento de datos personales. Por ello, los niveles de probabilidad e impacto deberán calcularse para cada caso concreto y no es posible hacerlo de una forma general en esta Guía.

En el Anexo II se incluye un posible modelo para ayudar a sistematizar y gestionar las fases de identificación y gestión de riesgos de una EIPD para su uso por aquellas organizaciones que así lo deseen.

7. CONSULTA CON LAS PARTES AFECTADAS

Las consultas con las partes afectadas, tanto internas como externas, son un tema que puede resultar delicado pero que es fundamental para el correcto desarrollo de una EIPD, especialmente cuando el proyecto evaluado tenga efectos sobre amplios sectores de la población y pueda generar desconfianza.

En concreto, las consultas son muy importantes para obtener la visión de personas u organizaciones que no están implicadas en el proyecto y que, por ello, lo pueden observar desde una perspectiva más amplia, poniendo de manifiesto riesgos que no son tan evidentes o pueden pasar desapercibidos para los que trabajan o están cercanos al mismo.

Por otra parte, hay que ser conscientes de que la consulta con las personas cuyos datos van a ser tratados o resultarán afectados por el proyecto es imprescindible pues, por una parte, posibilitará que la organización conozca las preocupaciones de los mismos y, por otra, dotará al proyecto de transparencia.

Entre estos terceros se incluyen desde organizaciones externas con las que se van a compartir datos personales o a las que se les van a entregar como representantes de los afectados y, en particular, de los colectivos cuyos datos van a ser tratados en el marco de los proyectos[21].

Para la realización de estas consultas no es necesario hacer públicos los planes detallados sobre los nuevos productos o servicios o revelar secretos comerciales o tecnológicos. Se pueden buscar alternativas para conseguir la opinión y la percepción de estos terceros mediante cuestionarios, reuniones o grupos de trabajo en los que, si es necesario, se requiera que los participantes estén vinculados por compromisos de confidencialidad.

[21] Asociaciones de usuarios, sindicatos, ONG dedicadas a la defensa de la privacidad, organizaciones sectoriales, etc.

Aunque las consultas pueden tener lugar en cualquier fase del proyecto e, incluso, desarrollarse de forma continuada a lo largo del mismo, no es conveniente posponerlas hasta las fases finales. Si durante las mismas se detectan riesgos que antes no habían sido identificados, su gestión puede resultar más costosa y compleja que si se hicieran en un momento anterior.

No obstante, tampoco es aconsejable llevar a cabo las consultas en fases muy iniciales, cuando el proyecto no esté todavía suficientemente definido y la información que se puede proporcionar a los distintos actores puede resultar fragmentaria o insuficientemente elaborada.

En el apartado interno, las consultas, dependiendo del proyecto y del tamaño de la organización y su estructura, podrían incluir a la dirección del proyecto y los técnicos implicados en el mismo, así como a los departamentos de TIC, compras, contratación, gestión de cobros, investigación del fraude, atención al público, comunicación, cumplimiento y gobernanza, las áreas de negocio afectadas y la alta dirección y, aunque no son estrictamente agentes internos, los encargados de tratamiento si los hubiere y aquellos proveedores cuya participación pudiera resultar relevante.

Si los tratamientos de datos personales previstos afectan a los empleados de la organización y, en particular, cuando entre sus finalidades se encuentren la vigilancia de sus actividades o el control laboral de los mismos, resultará imprescindible incluir en el proceso de consultas a los representantes de los trabajadores.

El alcance de la consulta dependerá de los tipos de riesgos y del número de personas afectadas, pero debe diseñarse para que la opinión de los afectados pueda influir en el proyecto. La consulta externa puede llevarse a cabo de diversas maneras, desde una consulta abierta a todas aquellas personas que quieran participar a la utilización de otras técnicas como *focus groups*, grupos de usuarios, reuniones públicas y sesiones con ciudadanos y consumidores, que pueden estarse ya usando en otros ámbitos de la organización y de cuya experiencia puede beneficiarse la EIPD.

Algunos elementos o principios que deberían tenerse en cuenta en cualquier tipo de consulta son los siguientes:

- Hacerla en el momento oportuno y dar el tiempo necesario para recibir las respuestas.
- Procurar que sea clara y proporcionada en temas y alcance.
- Facilitar que sea rica y representativa para asegurarse de que los afectados tengan voz.
- Hacer preguntas objetivas y presentar opciones realistas.
- Proporcionar información a los participantes sobre los resultados de la consulta al final del proceso.

8. GESTIÓN DE LOS RIESGOS IDENTIFICADOS

Una vez que se han identificado los riesgos del nuevo sistema, producto o servicio a través del análisis llevado a cabo por el equipo de la EIPD y tras atender a los resultados de las consultas internas y externas, llega el momento de gestionar dichos riesgos.

En la teoría general de análisis de riesgos se contemplan diversas opciones dependiendo del impacto que su materialización tendría para la organización: evitarlo o eliminarlo, mitigarlo, transferirlo o aceptarlo[22].

En algunos casos, estas opciones también estarán abiertas en relación con los riesgos para la privacidad identificados en una EIPD, pero en todos aquellos que supongan un incumplimiento normativo la única opción aceptable es evitarlos o eliminarlos.

Por ejemplo, si se está implantando un sistema de identificación biométrica se puede mitigar el riesgo de que terceros no autorizados accedan a la base de datos completa de plantillas biométricas utilizando un sistema descentralizado en el que las plantillas o los datos biométricos de cada persona se almacenen únicamente en una tarjeta inteligente que solo ella tendrá en su poder.

Pero si el riesgo detectado es, por ejemplo, la recogida de datos personales a través de cookies sin ofrecer la información establecida por la ley, la única opción posible es garantizar que se cumplirán los requerimientos legales de información y consentimiento inequívoco legalmente exigidos.

---

[22] Dado que existen múltiples metodologías de análisis de riesgos y todas ellas pueden resultar adecuadas para el objetivo buscado, no se incluyen en esta Guía directrices específicas en este ámbito. No obstante, por su relevancia y adaptación al caso específico de la privacidad, se puede hacer mención a la publicación Methodology for Privacy Risk Management de la Commission Nationale de l'Informatique et des Libertés (CNIL); a MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), herramienta creada por el Consejo Superior de Administración Electrónica para asistir a los distintos organismos públicos en este ámbito pero que es perfectamente utilizable también por el sector privado; Risk IT (ISACA) o ISO 27005. También pueden resultar útiles las normas ISO 31000 sobre principios y directrices de gestión del riesgo y la norma ISO 31010 sobre técnicas de gestión de riesgos, en la que se detallan diversos métodos que pueden ayudar a identificar y detectar los riesgos de un nuevo producto o servicio.

Es difícil detallar a priori un inventario completo de las posibles medidas que se pueden o deben adoptar para eliminar, mitigar o transferir los riesgos para la privacidad detectados en una EIPD puesto que dependen, en gran medida, de la naturaleza de los mismos y de cada proyecto específico.

A modo de ejemplo, a continuación se incluyen algunas medidas que se podrían adoptar para gestionar algunos riesgos que pueden haberse detectado en la fase anterior:

GENERALES	
Riesgos	**Medidas**
Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales	• Formación apropiada del personal sobre protección de datos • Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas de privacidad de la organización así como de las sanciones aparejadas al incumplimiento de las mismas
Pérdidas económicas y daños reputacionales derivados del incumplimiento de legislaciones sectoriales con incidencia en la protección de datos personales a las que pueda estar sujeto el responsable del tratamiento	• Formación apropiada del personal sobre protección de datos en el sector específico de que se trate • Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas de privacidad de la organización relativas a las legislaciones sectoriales que afectan a la organización, así como de las sanciones aparejadas al incumplimiento de las mismas
Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de las mismas, en particular, cuando se producen pérdidas de datos personales	• Formación apropiada del personal sobre seguridad y uso adecuado de las TIC • Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas y las medidas de seguridad así como de las sanciones aparejadas al incumplimiento de las mismas
Pérdida de competitividad del producto o servicio derivada de los daños reputacionales causados por una deficiente gestión de la privacidad de las personas	• Formación apropiada del personal sobre protección de datos, seguridad y uso adecuado de las TIC

GENERALES	
Riesgos	**Medidas**
Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados	• Nombrar a una persona o departamento como responsable de la interlocución con los afectados en todo aquello relativo a la privacidad y la protección de datos personales, y comunicar claramente la forma de contactar con ella • Nombrar un Delegado de Protección de Datos o Data Protection Officer (que dependiendo del tamaño de la organización será una persona o un departamento interno o externo) para ocuparse de todas las cuestiones relativas a la privacidad dentro de la organización y contar con asesoramiento cualificado. Si se procede a este nombramiento, el Delegado de Protección de Datos puede hacerse cargo también de la interlocución con los afectados
Incorporación tardía de los expertos en protección de datos (en particular, del delegado de protección de datos o DPO) al proyecto o definición deficiente de sus funciones y competencias	• Incluir dentro de los procedimientos de diseño y desarrollo de nuevos productos y servicios la incorporación del DPO en las fases iniciales de los mismos • Establecer desde la dirección las funciones, competencias y atribuciones del DPO en el desarrollo y gestión de los proyectos

LEGITIMACIÓN DE LOS TRATAMIENTOS Y CESIONES DE DATOS PERSONALES	
Riesgos	**Medidas**
Tratar datos personales cuando no es necesario para la finalidad perseguida	• Usar datos disociados siempre que sea posible y no implique un esfuerzo desproporcionado • Permitir el uso anónimo de los servicios y productos cuando no sea necesaria la identificación de las personas • Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso • Utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, sí que pueden contribuir a que la información sobre la identidad de los afectados solo sea accesible a un número reducido de personas • Evitar el uso de datos biométricos salvo que resulte imprescindible o esté absolutamente justificado
Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales	• Formación adecuada del personal sobre protección de datos, seguridad y uso adecuado de las TIC • Revisar las posibilidades que ofrece la legislación de protección de datos para permitir el tratamiento de datos personales y asegurar que este encaja en alguna de ellas • Si es necesario, buscar asesoramiento experto • Si se ceden datos personales, establecer por escrito acuerdos que contemplen las condiciones bajo las que se produce la cesión y, en su caso, las relativas a cesiones ulteriores así como las posibilidades de supervisión y control del cumplimiento del acuerdo

LEGITIMACIÓN DE LOS TRATAMIENTOS Y CESIONES DE DATOS PERSONALES	
Riesgos	**Medidas**
Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales	• Asegurarse de que no existen otras causas de legitimación más adecuadas • Cuando el tratamiento de datos personales se legitime por una relación contractual, ofrecer siempre la posibilidad de consentimiento separado para tratar datos con finalidades que no son necesarias para el cumplimiento o perfeccionamiento de la misma, evitando incluirlas de forma indisoluble en las cláusulas del contrato. • Evitar condicionar el disfrute de un producto o servicio al consentimiento para finalidades diferentes • En el ámbito laboral, evitar basar los tratamientos de datos en el consentimiento de los trabajadores • Evitar forzar el consentimiento desde una posición de prevalencia del responsable o cuando existen otras causas legitimadoras suficientes y más adecuadas
Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión	• Establecer procedimientos claros para manifestar la revocación del consentimiento o la solicitud de oposición a un determinado tratamiento. Si la organización realiza acciones publicitarias, tener en cuenta las reglas especiales existentes para las comunicaciones comerciales y, en particular, cuando estas se llevan a cabo a través de comunicaciones electrónicas • Establecer los mecanismos necesarios para garantizar que se consultan los ficheros de exclusión de publicidad, tanto de la organización como externos, y que se tienen en cuenta los deseos de quienes se han inscrito en ellos
Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros	• Exigir garantías de que los datos personales provenientes de terceros se han obtenido y cedido legal y lealmente. • En la realización de campañas publicitarias con datos provenientes de terceros en las que se segmenta el público objetivo en función de parámetros determinados, exigir garantías de que las personas cuyos datos van a ser utilizados han dado su consentimiento para ello

LEGITIMACIÓN DE LOS TRATAMIENTOS Y CESIONES DE DATOS PERSONALES	
Riesgos	**Medidas**
Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardias necesarias	• Verificar que el tratamiento de datos especialmente protegidos es absolutamente imprescindible para la finalidad o finalidades perseguidas • Verificar si el tratamiento está amparado o es requerido por una ley • En caso contrario, establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él
Enriquecer los datos personales de forma no prevista en las finalidades iniciales y sin la información adecuada a los afectados al realizar una interconexión con otras bases de datos de la organización o de terceros, en particular, la re-identificación de información disociada	• Verificar la legitimidad de la interconexión de datos prevista • Definir claramente los datos personales resultantes del tratamiento y verificar tras el proceso que son los únicos que se han generado
Utilizar cookies de seguimiento u otros mecanismos de rastreo sin obtener un consentimiento válido tras una información adecuada[23]	• Evitar el uso de cookies u otros mecanismos de rastreo y monitorización. En caso de que se utilicen, preferir las menos invasivas (cookies propias frente a cookies de terceros, cookies de sesión frente a cookies permanentes, periodos cortos de caducidad de las cookies, etc.) • Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas[24]. • Respetar las preferencias establecidas por los afectados en sus navegadores sobre el rastreo de su navegación
Impedir la utilización anónima de un determinado producto o servicio cuando la identificación del usuario no resulta indispensable	• Permitir el uso anónimo de los servicios y productos cuando no sea necesaria la identificación de las personas

[23] Ver *Guía sobre el uso de las cookies* de la Agencia Española de Protección de Datos redactada en colaboración con Adigital, Autocontrol e IAB. Canal de Publicaciones en www.agpd.es

[24] En el primer nivel se advertiría sobre el uso de cookies que se instalan al navegar o al utilizar el servicio solicitado y se identificarían sus finalidades, con información sobre si se trata de cookies propias o de terceros así como, en su caso, la advertencia de que si se realiza una determinada acción se entenderá que el usuario acepta el uso de las cookies. Además, habrá un enlace a una segunda capa que contendrá la definición y función de las cookies, los tipos de cookies que utiliza la página web y su finalidad, la forma de desactivar o eliminar las cookies descritas y forma de revocación del consentimiento ya prestado y la identificación de quienes instalan las cookies, incluidos los terceros con lo que el responsable haya contratado la prestación de un servicio que suponga el uso de cookies.

TRANSFERENCIAS INTERNACIONALES	
Riesgos	**Medidas**
Acceso secreto a los datos personales por parte de autoridades de terceros países	• Incluir cláusulas de salvaguarda en las que se requiera información sobre el acceso a los datos personales transferidos por parte de autoridades de terceros países tan pronto como sea posible
Carencia de mecanismos de control de cumplimiento de las garantías establecidas para la transferencia	• Si existen transferencias internacionales a países fuera del Espacio Económico Europeo, implantar los procedimientos de control necesarios (incluidos los contractuales) para garantizar que se cumplen las condiciones bajo las que se llevó a cabo la transferencia. En este sentido, hay que prestar especial atención cuando se contraten servicios de cloud computing u hospedados en terceros[25]
Impedimentos por parte del importador para el ejercicio de los procedimientos de supervisión y control pactados	• Asegurarse de la exigibilidad de mecanismos de control del importador tales como listas de encargados de tratamiento, países donde operan, posibilidad de revisar documentación y realizar auditorías, etc.
Incapacidad de ayudar a los ciudadanos en el ejercicio de sus derechos ante el importador	• Asegurarse de la definición y funcionamiento de un canal de comunicación entre exportador e importador para hacer llegar las solicitudes y reclamaciones de los afectados • Poner en marcha procedimientos que garanticen la adecuada atención de las demandas de los afectados
No obtención de las autorizaciones legales necesarias	• Solicitar la autorización del Director de la Agencia Española de Protección de Datos en aquellos casos que resulte necesario

NOTIFICACIÓN DE LOS TRATAMIENTOS	
Riesgos	**Medidas**
Carecer de los mecanismos y procedimientos necesarios para detectar cuándo debe notificarse la creación, modificación o cancelación de un tratamiento de datos personales a la AEPD o a la autoridad de protección de datos competente	• Incluir en los procesos y metodologías de desarrollo de nuevos proyectos una fase o tarea relativa a la revisión de la necesidad de notificar nuevos ficheros a la autoridad de control

[25] Ver las publicaciones de la Agencia Española de Protección de Datos *Guía para clientes que contraten servicios de Cloud Computing* y *Orientaciones para prestadores de servicios de Cloud Computing* disponibles en el Canal de Publicaciones en www.agpd.es

TRANSPARENCIA DE LOS TRATAMIENTOS	
Riesgos	**Medidas**
Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada (cookies, ubicación geográfica, comportamiento, hábitos de navegación, etc.)	• Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas[26]. • Establecer procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad, la homogeneidad de la información y, en particular, que se ofrece la información adecuada
En el entorno web, ubicar la información en materia de protección de datos (políticas de privacidad, cláusulas informativas) en lugares de difícil localización o diseminada en diversas secciones y apartados que hagan muy difícil su acceso conjunto y detallado	• Estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles fácilmente accesibles por los afectados y valorar la utilización de iconos u otros sistemas gráficos para facilitar su comprensión • Verificar que la información que se ofrece en todos los lugares y situaciones es coherente y sistemática • Verificar que la información se ofrece en todos los formularios
Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida que los afectados se hagan una idea clara y ajustada de los elementos esenciales que deben conocer para que exista un tratamiento leal de sus datos personales	• Implantar políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización

CALIDAD DE LOS DATOS	
Riesgos	**Medidas**
Solicitar datos o categorías de datos innecesarios para las finalidades del nuevo sistema, producto o servicio	• Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso

[26] En el primer nivel se advertiría sobre el uso de cookies que se instalan al navegar o al utilizar el servicio solicitado y se identificarían sus finalidades, con información sobre si se trata de cookies propias o de terceros así como, en su caso, la advertencia de que si se realiza una determinada acción se entenderá que el usuario acepta el uso de las cookies. Además, habrá un enlace a una segunda capa que contendrá la definición y función de las cookies, los tipos de cookies que utiliza la página web y su finalidad, la forma de desactivar o eliminar las cookies descritas y forma de revocación del consentimiento ya prestado y la identificación de quienes instalan las cookies, incluidos los terceros con lo que el responsable haya contratado la prestación de un servicio que suponga el uso de cookies.

CALIDAD DE LOS DATOS	
Riesgos	**Medidas**
Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados con informaciones diferentes o contradictorias, lo que puede derivar en la toma de decisiones erróneas	• Establecer medidas técnicas y organizativas que garanticen que las actualizaciones de datos de los afectados se comunican a todos los sistemas de información y departamentos de la organización que estén autorizados a utilizarlos
Garantías insuficientes para el uso de datos personales con fines históricos, científicos o estadísticos	• Siempre que sea posible, utilizar datos anónimos o disociados • Utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, sí que pueden contribuir a que la información sobre la identidad de los afectados solo sea accesible a un número reducido de personas • Garantizar que se aplican las medidas de seguridad adecuadas y correspondientes al nivel de seguridad de los datos utilizados
Utilizar los datos personales para finalidades no especificadas o incompatibles con las declaradas – Datos transaccionales, de navegación o de geolocalización para la monitorización del comportamiento, la realización de perfiles y la toma de decisiones sobre las personas – Toma de decisiones económicas, sociales, laborales, etc., relevantes sobre las personas (en particular las que pertenecen a colectivos vulnerables[27]) especialmente si pueden ser adversas o discriminatorias, incluyendo diferencias en los precios y costes de servicios y productos o trabas para el paso de fronteras – Toma de decisiones automatizadas con posibles consecuencias relevantes para las personas – Utilización de los metadatos para finalidades no declaradas o incompatibles con las declaradas	• Suministrar información transparente y clara sobre las finalidades para las que se tratarán los datos personales, en particular, a través de una política de privacidad visible y accesible • Proporcionar información sobre los criterios utilizados en la toma de decisiones y permitir a los afectados impugnar la decisión y solicitar que sea revisada por una persona • Proporcionar información sobre las medidas que se han implantado para lograr el necesario equilibrio entre el interés legítimo del responsable y los derechos fundamentales de los afectados

[27] Testigos protegidos, víctimas de violencia de género, menores, personas amenazadas, con nuevas identidades, desempleadas, dependientes, desfavorecidas o receptoras de asistencia social o sociosanitaria, discapacitadas, enfermas mentales o con enfermedades que generan rechazo social, etc.

CALIDAD DE LOS DATOS	
Riesgos	**Medidas**
Realizar inferencias o deducciones erróneas (y, en su caso, perjudiciales) sobre personas específicas mediante la utilización de técnicas de inteligencia artificial (en particular, minería de datos), reconocimiento facial o análisis biométricos de cualquier tipo	• Establecer mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer • Establecer posibilidades de impugnación ágiles para ofrecer vías de recurso adecuadas a los afectados • Establecer canales alternativos para tratar con los falsos negativos y falsos positivos en la identificación y autenticación de personas a través de datos biométricos
Carecer de procedimientos claros y de herramientas adecuadas para garantizar la cancelación de oficio de los datos personales una vez que han dejado de ser necesarios para la finalidad o finalidades para las que se recogieron	• Definir claramente los plazos de cancelación de todos los datos personales de los sistemas de información • Establecer controles automáticos dentro de los sistemas de información para avisar de la cercanía de los plazos de cancelación de la información • Implantar mecanismos para llevar a cabo y gestionar dicha cancelación en el momento adecuado incluyendo, si corresponde, el bloqueo temporal de los datos personales

DATOS ESPECIALMENTE PROTEGIDOS	
Riesgos	**Medidas**
Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso cuando éste sea la causa que legitima su tratamiento o cesión	• Evitar el uso de datos especialmente protegidos salvo que resulte absolutamente necesario • Establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él
Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos sensibles	• Nombrar un Delegado de Protección de Datos o Data Protection Officer (DPO) para contar con asesoramiento cualificado
Disociación deficiente o reversible que permita la re-identificación de datos sensibles en procesos de investigación que solo prevén utilizar datos anónimos	• Utilizar técnicas de disociación que garanticen el anonimato real de la información o, al menos, que el riesgo residual de re-identificación es mínimo

DEBER DE SECRETO	
Riesgos	**Medidas**
Accesos no autorizados a datos personales	• Establecer mecanismos y procedimientos de concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales • Establecer sanciones disciplinarias para quienes incumplan el deber de secreto y las políticas de confidencialidad de la organización • Establecer procedimientos que garanticen que se notifica formalmente a los trabajadores que acceden a datos personales de la obligación de guardar secreto sobre aquellos que conozcan en el ejercicio de sus funciones y de las consecuencias de su incumplimiento • Notificar que se dará traslado a las autoridades competentes de las violaciones de confidencialidad que puedan entrañar responsabilidades penales • Establecer procedimientos para garantizar la destrucción de soportes desechados que contengan datos personales
Violaciones de la confidencialidad de los datos personales por parte de los empleados de la organización	• Formación adecuada de los empleados sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información • Establecimiento de sanciones disuasorias para los empleados que violen la confidencialidad de los datos personales y comunicación clara y completa de las mismas

TRATAMIENTOS POR ENCARGO	
Riesgos	**Medidas**
Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas	• Establecer procedimientos que garanticen que siempre que se recurre a un encargado de tratamiento se firma el correspondiente contrato en los términos establecidos por la legislación de protección de datos

TRATAMIENTOS POR ENCARGO	
Riesgos	**Medidas**
Falta de diligencia (o dificultad para demostrarla) en la elección de encargado de tratamiento	• Seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento de los contratos y de la adopción de las medidas de seguridad estipuladas a través, por ejemplo, de su adhesión a posibles códigos de conducta o a esquemas de certificación homologados y de acreditada solvencia • Establecer contractualmente mecanismos de supervisión, verificación y auditoría de los tratamientos encargados a terceros
Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad	• Establecer mecanismos y procedimientos que garanticen el control sobre las actividades de los subcontratistas que pueda elegir un encargado de tratamiento • Realizar auditorías periódicas al encargado de tratamiento para verificar que cumple las estipulaciones del contrato • Definir acuerdos de nivel de servicio que garanticen el correcto cumplimiento de las instrucciones del responsable y la adopción de las medidas de seguridad adecuadas
No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos ARCO realizados ante los encargados de tratamiento	• Incluir en el contrato de encargo la obligación de comunicar al responsable las peticiones de ejercicio de los derechos ARCO • Definir los procedimientos operativos para que esta comunicación se lleve a cabo de forma ágil y eficiente
Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato	• Incluir la obligación de portabilidad en el contrato y en los acuerdos de nivel de servicio • Establecer medidas técnicas y organizativas que garanticen la portabilidad

DERECHOS ARCO	
Riesgos	**Medidas**
Dificultar o imposibilitar el ejercicio de los derechos ARCO	• Implantar sistemas que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos ARCO • Evitar sistemas de ejercicio de los derechos ARCO que impliquen solicitar una remuneración • Evitar establecer procedimientos poco transparentes, complejos y laboriosos • Formar a todo personal para que conozca qué ha de hacer si recibe una petición de derecho ARCO o ha de informar a los afectados sobre cómo ejercerla • Definir qué personas o departamentos se ocuparán de gestionar los derechos ARCO y formarlos adecuadamente
Carencia de procedimientos y herramientas para la gestión de los derechos ARCO	• Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen que todos los empleados conocen cómo actuar ante un ejercicio de derechos ARCO y que pueden suministrar la información adecuada a los afectados • Formación de los empleados encargados de gestionar los ejercicios de derechos ARCO
Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales	• Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate • Establecimiento de acuerdos y procedimientos de gestión y comunicación con los cesionarios de la información que garanticen la correcta actualización de los datos personales cedidos • Formación de los empleados encargados de gestionar los ejercicios de derechos ARCO

SEGURIDAD	
Riesgos	**Medidas**
Inexistencia del responsable de seguridad o deficiente definición de sus funciones y competencias	• Nombramiento del responsable de seguridad y establecimiento por parte de la dirección de sus funciones, competencias y atribuciones en el desarrollo y gestión de los proyectos • Incluir dentro de los procedimientos de diseño y desarrollo de nuevos productos y servicios la incorporación del responsable de seguridad en las fases iniciales de los mismos
Deficiencias organizativas en la gestión del control de accesos	• Políticas estrictas de *need to know* (necesidad de conocer o acceder a la información) para la concesión de accesos a la información y de *clean desks* (escritorios limpios) para minimizar las posibilidades de acceso no autorizado a los datos personales • Establecer procedimientos que garanticen la revocación de permisos para acceder a datos personales cuando ya no sean necesarios (abandono de la organización, traslado, cambio de funciones, etc.) • Inventariar los recursos que contengan datos personales accesibles a través de redes de telecomunicaciones
Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales	• Instalar herramientas de hardware o software que ayuden a una gestión eficaz de la seguridad y los compromisos u obligaciones legales de la organización en el área de la protección de datos personales • En el caso de que pudiera resultar necesario, instalar herramientas de detección de intrusiones (*Intrusion Detection Systems*) y/o de prevención de intrusiones (*Intrusion Prevention Systems*) con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad • En la medida que pudiera resultar necesario, implantar sistemas de *Data Loss Prevention* o Prevención de Pérdida de Datos con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad

SEGURIDAD	
Riesgos	**Medidas**
Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información	• Establecer mecanismos de registro de acciones sobre los datos personales o *logging* así como herramientas fiables y flexibles de explotación de los ficheros de auditoría resultantes
Uso de identificadores que revelan información del afectado	• Establecer políticas de asignación de códigos de usuario por parte de la organización que eviten datos triviales como fecha de nacimiento, nombre y apellidos, etc. • Evitar el uso de identificadores ligados a elementos de autenticación, como números de tarjetas de crédito o similares, ya que favorecen el fraude en la identificación e incluso la suplantación de identidad
Deficiencias en la protección de la confidencialidad de la información	• Adoptar medidas de cifrado –adecuadas al riesgo y al estado de la tecnología– de los datos personales almacenados y compartidos a través de redes de telecomunicaciones (en particular, si son públicas y/o inalámbricas) para minimizar el riesgo de que terceros no autorizados accedan a ellos ante un hipotético fallo de seguridad • Establecer procedimientos de notificación a las personas afectadas para el caso en que sus datos hayan podido ser accedidos o sustraídos por terceros no autorizados, informándoles de las medidas que pueden utilizar para minimizar los riesgos • Establecer procedimientos de notificación de quiebras de seguridad a la autoridad de control cuando ello sea legalmente exigible • Evitar, en general, las pruebas con datos reales y, en particular, cuando incluyan datos especialmente protegidos o un conjunto importante de datos que revelen aspectos relevantes de la personalidad de los afectados, cuando se empleen los de muchas personas o cuando participen en las pruebas un número elevado de usuarios • Construir canales seguros y con verificación de identidad para la distribución de información de seguridad (códigos de usuario, contraseñas, etc.)

SEGURIDAD	
Riesgos	**Medidas**
Falta de formación del personal sobre las medidas de seguridad que están obligados a adoptar y sobre las consecuencias que se pueden derivar de no hacerlo	• Formación sobre la política de seguridad de la organización y, en particular, sobre las obligaciones de cada empleado • Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas y las medidas de seguridad, así como de las sanciones aparejadas al incumplimiento de las mismas
Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc.) para terceros no autorizados	• En el caso de que pudiera resultar necesario, instalar herramientas de detección de intrusiones (*Intrusion Detection Systems*) y/o de prevención de intrusiones (*Intrusion Prevention Systems*) con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad • En la medida que pudiera resultar necesario, implantar sistemas de *Data Loss Prevention* o Prevención de Pérdida de Datos con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad

En el caso particular de que el tratamiento se justifique por el interés legítimo del responsable del mismo o del cesionario o cesionarios de la información, habrá de poner un cuidado especial, primero, en la valoración de si el tratamiento no afecta derechos fundamentales de los afectados y, a continuación, en la implantación de las medidas de salvaguardia adecuadas para garantizar que se logra el equilibrio entre los intereses del responsable y los derechos de las personas.

Para finalizar esta sección hay que resaltar que es imprescindible la monitorización continua de que las medidas de gestión del riesgo adoptadas son efectivas y cumplen el objetivo para el que fueron implantadas y, en caso de no ser así, introducir los cambios y modificaciones que resulten necesarias para conseguir los objetivos perseguidos.

9. ANÁLISIS DE CUMPLIMIENTO NORMATIVO

Uno de los aspectos decisivos en toda Evaluación de Impacto en la Protección de Datos (EIPD) es el relativo a la verificación de la conformidad del proyecto con las distintas regulaciones que pueden contener elementos relativos a la privacidad y a la protección de datos que le sean de aplicación.

Ello incluye la legislación básica de protección de datos personales y, en concreto, la Ley Orgánica de Protección de Datos y su Reglamento de Desarrollo. Pero, dependiendo del sector en el que opere la organización o del proyecto concreto, también pueden existir obligaciones adicionales como, por ejemplo, la legislación sanitaria, de telecomunicaciones o de servicios de sociedad de la información o, en la propia LOPD, lo que se refiere a los ficheros de las Fuerzas y Cuerpos de Seguridad, a la prestación de servicios de solvencia patrimonial y crédito, o los tratamientos con fines de publicidad y prospección comercial.

Para facilitar la realización de este análisis, en el Anexo I de esta Guía se han incluido una serie de cuestiones a las que sería necesario dar respuesta para comprobar si los tratamientos de datos personales que estamos analizando respetan los principios y derechos establecidos en la Ley Orgánica 15/1999 y su Reglamento de Desarrollo, sin abordar la revisión de otras normas que pudieran resultar de aplicación.

10. REDACCIÓN, PUBLICACIÓN E INTEGRACIÓN DEL INFORME FINAL

El equipo encargado de llevar a cabo la EIPD debe prestar una gran atención a la presentación de sus conclusiones a través de su informe final, que debería hacerse público (de forma completa o parcial si existen apartados que no pueden ser divulgados por restricciones legales, comerciales o de seguridad), por ejemplo, a través del sitio web de la organización.

Aunque esta Guía no pretende establecer un modelo único de informe ya que, según las herramientas utilizadas por las organizaciones en la gestión de sus proyectos, podrían tener otros formatos que resultaran adecuados, la AEPD considera que hay un conjunto de apartados que no deberían faltar:

- Identificación clara del proyecto, la persona o personas responsables de la EIPD y sus datos de contacto, la fecha de realización del informe y número de versión del mismo.
- Resumen del informe con los resultados esenciales escrito con claridad y concisión.
- Introducción y descripción general del proceso de evaluación para aquellos lectores que no estén familiarizados con esta técnica.
- Resultado del análisis de necesidad de la evaluación y su justificación.
- Descripción general del proyecto con el nivel de detalle necesario (se pueden incluir como anexos los documentos relevantes del proyecto que se juzguen oportunos).
- Descripción detallada de los flujos de datos personales.
- Riesgos identificados.
- Identificación de partes interesadas o a las que afecta el proyecto, tanto internas como externas a la organización, y resultados de las consultas llevadas a cabo con las mismas.

- Análisis de cumplimiento normativo y, en particular, detalle de posibles deficiencias detectadas y propuestas para su solución.
- Recomendaciones del equipo responsable de la EIPD y enumeración de las medidas adoptadas o que deben adoptarse en el diseño del proyecto para eliminar o evitar, mitigar, transferir o aceptar los riesgos para la privacidad[28] incluidas las de carácter organizativo.

Además de estos puntos, cada organización podrá incluir otros apartados que considere necesarios o convenientes para una mejor información de la alta dirección y el resto de destinatarios del informe como, por ejemplo, un análisis coste-beneficios de las distintas medidas recomendadas en el informe o cualesquiera otros que se juzguen adecuados.

Finalmente, el lenguaje del informe debe ser lo más claro y transparente posible, huyendo de tecnicismos tanto legales como tecnológicos, permitiendo su comprensión a todos los destinatarios del mismo o, al menos, si no es posible dejar de evitar ciertos términos jurídicos o tecnológicos, es conveniente incluir un glosario con las definiciones y no dar por supuesto que cualquier lector los conoce con precisión.

En el Anexo III se incluye un posible modelo de informe final de una EIPD para su utilización por parte de aquellas organizaciones que así lo deseen.

[28] Como ya se ha mencionado, cuando los riesgos suponen un incumplimiento normativo la única opción posible es eliminarlos o evitarlos.

11. IMPLANTACIÓN DE LAS RECOMENDACIONES

El informe final del equipo de la EIPD debe ser remitido a la alta dirección de la organización para que tome las decisiones necesarias en relación con las recomendaciones realizadas y las medidas sugeridas.

Esta remisión tiene dos motivos. El primero de ellos es que la dirección defina y tome las decisiones necesarias para poner en marcha los cambios o mejoras que hubieran de ser introducidas en el proceso tomando como base las sugerencias realizadas en el informe.

En segundo lugar, debe establecer la persona o unidad responsable de coordinar que se implanten las medidas recomendadas y, para que su labor resulte eficaz, investirla de la necesaria autoridad para realizar su trabajo, y comunicar a la dirección los avances y dificultades que encuentre en el mismo.

Como las medidas a adoptar pueden ser de muy diversos tipos (organizativas, tecnológicas, contractuales, etc.) no existe un método que indique cómo han de ser llevadas a cabo, y cada organización debe decidir cuál es el que mejor se adapta a su cultura y estructuras de gestión.

Otro aspecto importante es el referente a aquellas medidas que deben ser adoptadas por un proveedor externo. En estos casos, aparte de las posibles modificaciones contractuales que pudieran resultar necesarias, también habría que prever los mecanismos de control y supervisión que se deben definir y adoptar para garantizar que estos terceros realmente implantan las medidas acordadas.

12. REVISIÓN DE LOS RESULTADOS Y REALIMENTACIÓN DE LA EVALUACIÓN DE IMPACTO

Una vez que se han obtenido los resultados de la EIPD y se han implantado las medidas correctoras y de mejora adoptadas por la alta dirección de la organización llega el momento de la revisión y comprobación de su implantación real y de su eficacia.

Es necesario, pues, examinar el proyecto una vez operativo para verificar que los riesgos detectados se han abordado correctamente y que no existen otros nuevos que en su momento pasaron desapercibidos o que han surgido posteriormente, lo que llevaría aparejada una nueva iteración de las fases de la EIPD.

Por ello, una evaluación de impacto, aunque tiene una importancia y un protagonismo especial en las fases iniciales de un proyecto, es un proceso que acompaña al sistema de información, producto o servicio durante todo su ciclo de vida.

Y, por supuesto, la modificación del mismo o la incorporación de nuevas funcionalidades deberán llevar consigo la necesidad de revisar la EIPD con un alcance mayor o menor en función de la profundidad y magnitud de los cambios introducidos.

Así, el esquema clásico de la Rueda o Ciclo de Deming (planificar, implantar, verificar y actuar) también deberá ser observado en la realización y desarrollo de las EIPD.

13. CONCLUSIÓN

Las Evaluaciones de Impacto en la Protección de Datos Personales son una herramienta nueva en España pero cuentan ya con una tradición de décadas, fundamentalmente en países de habla inglesa. La AEPD entiende que son instrumentos que pueden jugar un papel fundamental en la mejora de la privacidad en todos aquellos nuevos tratamientos de datos personales que se pongan en marcha.

Las evaluaciones de impacto en la protección de datos personales forman parte esencial de una nueva generación de herramientas y metodologías que buscan una aproximación proactiva a los retos de implantar garantías que salvaguarden el derecho fundamental a la protección de datos en nuestras modernas sociedades de la información, constituyéndose, además, en un elemento destacado de la Privacidad desde el Diseño.

Igualmente, cada vez se abre paso con más fuerza la idea de que los responsables de tratamientos de datos personales han de ser capaces de demostrar su compromiso con los derechos de los ciudadanos y el cumplimiento de sus obligaciones legales (*accountability)*. En este sentido, una EIPD desarrollada con seriedad es un instrumento ideal para que los responsables puedan mostrar esa diligencia y desarrollar los métodos y procedimientos adecuados.

La Agencia Española de Protección de Datos confía en que esta Guía promueva la concienciación de las organizaciones y que impulse y estimule la utilización de esta herramienta para conseguir que la protección de datos personales sea, cada vez más, parte indisoluble de la cultura de entidades públicas y privadas y que, de esta manera, se contribuya a la creación de confianza entre los ciudadanos, confianza que tan necesaria resulta para el despegue y correcto funcionamiento de los servicios de la Sociedad de la Información.

14. REFERENCIAS

[1] Stewart, B. Privacy impact assessments. Privacy Law and Policy Reporter. Australia (1996)

[2] Clarke, R. Privacy Impact Assessment: Its Origins and Developments. Computer Law & Security Review (2009)

[3] Wright, D., De Hert, P. Privacy Impact Assessment. Springer (2012)

[4] Privacy Impact Assessment Handbook. Office of the Information Commissioner. Reino Unido (2009)

[5] Conducting privacy impact assessments code of practice. Office of the Information Commissioner. Reino Unido (2014)

[6] Privacy Impact Assessment Handbook. New Zealand Privacy Commissioner. Nueva Zelanda (2007)

[7] Recommendations for a privacy impact assessment framework for the European Union. Proyecto «Privacy Impact Assessment Framework». Bruselas-Londres (2012)

[8] Privacy and Data Protection Impact Assessment Framework for RFID Applications. Bruselas (2011)

[9] Privacy Impact Assessments. A guide for the Victorian Public Sector; Accompanying Guide Report and Report Template. Victoria-Australia (2009)

[10] Dictamen 9/2011 relativo a la Propuesta Revisada de la Industria para un Marco de Evaluación del Impacto sobre la Protección de Datos y la Intimidad en las Aplicaciones Basadas en la Identificación por Radiofrecuencia (RFID). Grupo de Trabajo del Artículo 29. Bruselas (2011)

[11] Methodology for Privacy Risk Management. Commission Nationale de l'Informatique et des Libertés (CNIL). París (2012)

[12] Template for a PIA report. Proyecto «Privacy Impact Assessment Framework». Bruselas-Londres (2012)

[13] Metodología para el Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) Versión 3. Consejo Superior de Administración Electrónica (2012)

[14] Risk IT. Marco de riesgos de TI. ISACA (2009)

[15] ISO/IEC 27005:2011 Information Technology. Security Techniques. Information security risk management. ISO (2011).

[16] UNE-ISO 31000:2010. Gestión del riesgo. Principios y directrices. AENOR (2010)

[17] UNE-ISO 31010:2011. Gestión del riesgo. Técnicas de apreciación del riesgo. AENOR (2011)

[18] The Orange Book. Management of Risk - Principles and Concepts. HM Treasury. Reino Unido (2004)

15. ANEXO I. GUÍA PARA UN ANÁLISIS DE CUMPLIMENTO NORMATIVO

A continuación se presenta un conjunto de cuestiones básicas que habrán de responderse para determinar si existen aspectos de cumplimiento de la ley que no se han tenido en cuenta en el proyecto, al objeto de hacer un repaso que deberá ser de mayor o menor profundidad en función de las características del mismo. A este respecto, hay que señalar que la Agencia Española de Protección de Datos ha desarrollado la herramienta Evalúa para ayudar a los responsables de ficheros a revisar su grado de cumplimiento de la legislación de protección de datos. Evalúa está disponible en la página web de la AEPD y puede servir de gran ayuda en este apartado.

LEGITIMACIÓN DE LOS TRATAMIENTOS Y LAS CESIONES DE DATOS PERSONALES

- ¿Se cuenta con el consentimiento libre, específico, inequívoco e informado de los afectados para el tratamiento de sus datos personales?
- En caso contrario, ¿se da alguna de las siguientes circunstancias?
  - **a.** ¿Está autorizado por una ley?
  - **b.** ¿Se deriva del ejercicio de competencias propias de las AA. PP.?
  - **c.** ¿Responde a una relación negocial, contractual, laboral o administrativa?
  - **d.** ¿Se debe a un interés vital del afectado?
  - **e.** ¿Proceden los datos de fuentes accesibles al público?

f. ¿Es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección? En este caso, ¿se ha realizado un análisis exhaustivo y una ponderación rigurosa entre los intereses del responsable y los derechos de los ciudadanos? ¿Se han establecido medidas de garantía y salvaguardia para limitar los efectos del tratamiento sobre los afectados?

g. ¿Está asociado al ejercicio de un derecho fundamental (libertad de expresión, libertad de información, tutela judicial efectiva, libertad sindical, etc.)? ¿Prevalece este derecho sobre el derecho a la protección de datos personales?

- En el caso de que el tratamiento se base en el consentimiento del afectado, ¿existen mecanismos para probar que se ha prestado en los términos que marca la ley y para que se pueda ejercer la revocación del mismo?
- ¿Se cuenta con el consentimiento libre, específico, inequívoco e informado de los afectados para la cesión de sus datos personales?
- En caso contrario, ¿se da alguna de las siguientes circunstancias?

  a. ¿Está autorizada por una ley?

  b. ¿Se deriva de libre y legítima aceptación de una relación jurídica que la exija?

  c. ¿Tiene como destino al Defensor del Pueblo, el Ministerio Fiscal, los Jueces o Tribunales o el Tribunal de Cuentas u organismos autonómicos similares?

  d. ¿Se realiza entre AA. PP. para el ejercicio de competencias similares o para el tratamiento posterior para fines científicos, históricos o estadísticos?

  e. ¿Es necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos conforme a su legislación específica?

  f. ¿Proceden los datos de fuentes accesibles al público?

  g. ¿Es necesario para la satisfacción del interés legítimo perseguido por el tercero o terceros a los que se comuniquen los datos siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección? En este caso, ¿se ha realizado un análisis riguroso y una ponderación rigurosa entre los intereses del responsable y los derechos de los ciudadanos? ¿Se han establecido medidas de garantía y salvaguardia para limitar los efectos de la cesión sobre los afectados?

- ¿Se informa de la finalidad a la que se destinarán los datos o del tipo de actividad del cesionario?
- ¿Se está en condiciones de acreditar el consentimiento obtenido?
- ¿Se han habilitado procedimientos para gestionar la revocación del consentimiento del afectado?

TRANSFERENCIAS INTERNACIONALES

- ¿Se van a transferir datos personales fuera de España?
- ¿Es el país de destino un miembro del Espacio Económico Europeo?
- Si no es así, ¿es un país declarado adecuado por la Comisión Europea o el Director de la AEPD?
- En caso contrario, ¿se puede aplicar alguna de las excepciones previstas por la LOPD en su artículo 34?
- Si no se está en ningún caso anterior, ¿se ha solicitado la preceptiva autorización del Director de la Agencia Española de Protección de Datos a través de los instrumentos jurídicos reconocidos a este fin (cláusulas contractuales tipo aprobadas por la Comisión Europea o el Director de la AEPD, Normas Corporativas Vinculantes, etc.)?
- Si se trata de un encargado de tratamiento que desea subcontratar servicios a terceros por cuenta de sus clientes, ¿se hace uso de las cláusulas contractuales tipo aprobadas por la Agencia Española de Protección de Datos? En caso contrario, cada responsable debería de solicitar la correspondiente autorización.

NOTIFICACIÓN DE LOS TRATAMIENTOS A LA AEPD

- ¿Se han seguido los pasos necesarios para notificar al Registro General de Protección de Datos de la AEPD los ficheros o tratamientos de datos personales?
- En el caso de que el responsable sea una Administración Pública, ¿se ha publicado la disposición de carácter general en el diario oficial correspondiente?

TRANSPARENCIA DE LOS TRATAMIENTOS

- ¿Se informa a los afectados expresa e inequívocamente de la existencia de un tratamiento de datos personales, de la identidad y dirección del responsable del tratamiento, de su finalidad, de los destinatarios de los datos, de la obligatoriedad o no de las respuestas y de las consecuencias de no prestarlas y de la posibilidad de ejercer los derechos ARCO?
- ¿Figura la anterior información en los formularios, tradicionales o electrónicos, de recogida de información?
- Si los datos no se recaban directamente de los afectados, ¿se informa a los mismos, en el plazo de tres meses desde el registro de los datos personales, de forma expresa e inequívoca de la existencia de un tratamiento de datos personales, de la identidad y dirección del responsable del tratamiento, de su finalidad, de los destinatarios de los datos y de la posibilidad de ejercer los derechos ARCO?

CALIDAD DE LOS DATOS

- ¿Se recogen solo los datos personales estrictamente necesarios para las finalidades de que se trate?
- ¿Se recaban los datos de forma leal y transparente?
- ¿Se usan los datos para finalidades distintas o incompatibles con las establecidas y comunicadas al afectado?
- ¿Se adoptan, en su caso, las garantías necesarias para el tratamiento de datos con finalidades históricas, científicas o estadísticas?
- ¿Existen mecanismos de actualización de la información y de verificación de dicha actualización?
- ¿Se contempla la posibilidad de cancelar los datos personales de oficio, cuando ya no sean necesarios para la finalidad o finalidades para las que se recogieron?
- ¿Se definen los plazos de conservación de los datos personales? ¿Existen procedimientos para determinar que se han cumplido los plazos máximos de conservación de los datos personales?

- ¿Se conservan los datos personales de manera que puedan ejercerse los derechos ARCO?
- En el caso de que se proceda a disociar los datos personales, ¿se utilizan procedimientos que garantizan la irreversibilidad del proceso y la imposibilidad de re-identificar a los titulares de los datos?

DATOS ESPECIALMENTE PROTEGIDOS

- Si se tratan datos especialmente protegidos de ideología, religión, creencias o afiliación sindical, ¿se cuenta con el consentimiento expreso y por escrito?
- Si se tratan datos especialmente protegidos de salud, vida sexual u origen racial o étnico, ¿se cuenta con el consentimiento expreso? En caso contrario, ¿existe una ley que permita su tratamiento?
- ¿Se está en condiciones de acreditar el consentimiento expreso obtenido?
- ¿Se han habilitado procedimientos para gestionar la revocación del consentimiento expreso del afectado?
- ¿Se recogen datos de infracciones penales o administrativas sin ser el órgano competente?
- En el caso de tratamientos de datos especialmente protegidos para la prestación o gestión de servicios sanitarios, ¿se garantiza adecuadamente el deber de secreto de todas las personas que tienen acceso a ellos? ¿Se limita el acceso a los datos de salud a los estrictamente necesarios para cada una de las diferentes funciones (sanitarias, administrativas, investigadoras, docentes, etc.) que se llevan a cabo?

DEBER DE SECRETO

- ¿Se forma adecuadamente a todas las personas que tratan datos de carácter personal de la obligación de guardar secreto sobre los datos que conozcan en el ejercicio de sus funciones?
- ¿Se les informa adecuadamente de sus obligaciones y de las consecuencias de no hacerlo? ¿Queda constancia de dicha información?

TRATAMIENTOS POR ENCARGO

- ¿Se han realizado los análisis necesarios de manera diligente para elegir un encargado de tratamiento que ofrezca las garantías adecuadas?
- ¿Se regula la relación entre el responsable y el encargado en un contrato (escrito o acordado electrónicamente con las garantías que establece la ley)?
- ¿Se han adoptado medidas para verificar el cumplimiento de las condiciones contractuales y de las medidas de seguridad por parte del encargado y de los posibles subcontratistas?
- ¿Se estipula que el encargado solo podrá tratar los datos personales conforme a las instrucciones del responsable y no los aplicará a fines distintos?
- ¿Se estipula que los datos no serán comunicados a otras personas?
- ¿Se estipulan las medidas de seguridad que deberá adoptar el encargado?
- ¿Se regula el destino de los datos personales a la finalización de la prestación de que se trate (destrucción, devolución al responsable o comunicación a otro encargado designado por el responsable)?
- ¿Se informa al encargado de que en caso de que destine los datos a otra finalidad, los comunique o incumpla el contrato será considerado responsable y podrá incurrir en el régimen sancionador de la LOPD?
- ¿Existe una cesión porque el encargado del tratamiento establece un nuevo vínculo con los afectados?
- Si existen o van a existir subcontrataciones, ¿se cuenta con la autorización del responsable?
- Si no existe dicha autorización, ¿se han especificado en el contrato los servicios que pueden ser objeto de subcontratación y la empresa con la que se va a subcontratar? En su defecto, ¿se comunica al responsable la empresa subcontratada cuando se lleve a efecto la subcontratación? ¿Se ajusta el subcontratista a las instrucciones del responsable? ¿Se formaliza un contrato entre encargado y subcontratista en los términos del contrato inicial?
- Si el encargado de tratamiento presta sus servicios en los locales del responsable o bien accede remotamente a los datos personales sin posibilidad de copiarlos o incluirlos en sus sistemas, ¿se ha reflejado este hecho en el documento de seguridad del responsable? ¿Se

ha comprometido el personal del encargado a cumplir las medidas de seguridad establecidas por el responsable?

- En el caso de que la prestación no implique acceso a datos personales, ¿se recoge expresamente la prohibición de acceder a datos personales y la obligación de secreto sobre aquellos que el encargado incidentalmente hubiera podido conocer?
- Si el servicio se presta en los locales del encargado de tratamiento, ¿se ha incluido este hecho en su documento de seguridad así como la identidad del responsable del tratamiento? ¿Ha desarrollado el encargado del tratamiento el documento de seguridad correspondiente o completado el que ya tuviera con la información referida al encargo recibido?

DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN (DERECHOS ARCO)

- ¿Se adoptan las medidas necesarias para garantizar el carácter personalísimo (verificación de la identidad o, en su caso, de la validez de la representación otorgada a un tercero) del ejercicio de los derechos?
- ¿Se han adoptado medidas para acreditar la representación en casos de incapacidad o minoría de edad?
- ¿Se ha previsto el ejercicio de los derechos ARCO mediante representante voluntario y la forma de acreditar dicha representación?
- ¿Se ha habilitado un medio sencillo y gratuito para el ejercicio de los derechos ARCO?
- Si el responsable dispone de servicios de atención al público o de gestión de reclamaciones, ¿se concede la posibilidad de utilizar estos servicios para ejercer los derechos ARCO y se considera acreditada la identidad de los interesados mediante los medios establecidos por el responsable para la prestación de estos servicios?
- ¿Se conservan los datos personales de tal forma que permitan el fácil y rápido ejercicio de los derechos?
- ¿Se han implantado las medidas y procedimientos adecuados para garantizar el ejercicio de los derechos ARCO en los plazos marcados por la ley?

- En el caso de que el responsable utilice encargados de tratamiento, ¿les ha instruido para que le den traslado de cualquier ejercicio de derechos que reciba salvo que en la relación entre ambos se contemple que el encargado atienda también los derechos ARCO?
- ¿Se han implantado las medidas y procedimientos adecuados para que siempre se proporcione una respuesta a los ciudadanos que ejercen estos derechos?
- ¿Se han implantado medidas y procedimientos para responder a los requerimientos de la AEPD en el marco de los procedimientos de tutela de derechos?
- ¿Existen mecanismos y procedimientos para informar a los posibles cesionarios de datos personales de las rectificaciones o cancelaciones realizadas?
- En el caso del derecho de acceso, ¿se ofrece toda la información que establece la ley y en los formatos adecuados y legibles sin tener que recurrir a medios adicionales para su interpretación? ¿Se garantiza que el derecho se pueda ejercer a intervalos superiores a doce meses o cuando se acredite un interés legítimo para hacerlo en un plazo menor?
- En el caso del derecho de cancelación, ¿se conservan los datos personales durante los plazos previstos por las disposiciones aplicables o en las relaciones contractuales y solo por esos plazos? ¿Se mantienen los datos bloqueados a disposición de las AA. PP., los Jueces y Tribunales durante el plazo de prescripción de responsabilidades?
- En el caso de que se adopten decisiones con efectos jurídicos basadas únicamente en un tratamiento automatizado de datos personales, ¿se han previsto los mecanismos necesarios para que dichas decisiones puedan ser impugnadas por los afectados? ¿Se han habilitado procedimientos para dar información sobre los criterios de valoración y el programa utilizado a petición de los afectados?

SEGURIDAD

GENERAL

- ¿Se ha llevado a cabo la clasificación e identificación del nivel de seguridad (básico, medio o alto) que deben satisfacer todos y cada uno de los ficheros o tratamientos de datos personales?

- ¿Se garantiza que las medidas de seguridad para el acceso a datos personales a través de redes de telecomunicaciones garantizan el mismo nivel de seguridad que el existente en el entorno local?
- ¿Existe un procedimiento para gestionar las autorizaciones para la salida de dispositivos portátiles que contienen datos personales fuera de los locales del responsable?
- ¿Cumplen las copias de trabajo y los ficheros temporales las medidas de seguridad correspondientes a su nivel? ¿Se destruyen una vez han dejado de ser necesarios?
- ¿Se ha elaborado el preceptivo documento de seguridad (DS)?

SEGURIDAD FICHEROS AUTOMATIZADOS

NIVEL BÁSICO

- ¿Se han definido claramente en el DS las funciones y obligaciones de los usuarios que acceden a los sistemas de información que contienen datos personales?
- ¿Se han establecido los procedimientos necesarios para que todo el personal conozca las medidas de seguridad que le afectan y que debe implantar?
- ¿Se ha creado un registro de incidencias y un procedimiento para su gestión? ¿Se ha difundido este procedimiento para conocimiento general de todo el personal?
- ¿Se ha asegurado que cada usuario acceda únicamente a los datos personales que son necesarios para sus funciones?
- ¿Existe una relación actualizada de perfiles con estas autorizaciones y los mecanismos para su actualización?
- ¿Existen medidas para evitar que un usuario acceda a recursos con permisos distintos de los autorizados?
- ¿Está claramente delimitado y consignado en el DS el personal autorizado para gestionar estos permisos?
- ¿Existen medidas adecuadas para identificación, inventario, control de acceso y autorización de la salida de soportes?

- ¿Se han adoptado las medidas adecuadas para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte?
- ¿Existen medidas para evitar que los soportes desechados contengan datos personales que puedan ser recuperados?
- ¿Existen medidas para garantizar la correcta identificación y autenticación de los usuarios de forma inequívoca y personalizada?
- ¿Existe un procedimiento seguro de asignación, distribución y almacenamiento de contraseñas?
- ¿Existen procedimientos para el cambio periódico de contraseñas (al menos una vez al año)?
- ¿Existen mecanismos de realización de copias de seguridad y de recuperación de la información que contienen?
- ¿Se verifica cada seis meses el correcto funcionamiento de estos sistemas?
- Si se realizan pruebas con datos reales, ¿se garantiza que se protegen con las medidas de seguridad acordes con su nivel de seguridad? ¿Se asegura que se hace una copia con carácter previo a su utilización?

NIVEL MEDIO

Además de las del Nivel Básico:

- ¿Se ha designado un responsable o responsables de seguridad?
- ¿Se realizan auditorías bienales o cada vez que se produzcan modificaciones sustanciales en los sistemas de información?
- ¿Se ha establecido un sistema de registro de entrada y salida de soportes y documentos?
- ¿Existe un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información?
- ¿Existe control de acceso físico a los locales donde están ubicados los equipos físicos que dan soporte a los sistemas de información?
- ¿Existen procedimientos para consignar en el registro de incidencias los mecanismos de recuperación que haya sido necesario ejecutar?

NIVEL ALTO

Además de las del Nivel Básico y Medio:

- ¿Existen procedimientos y herramientas para cifrar los soportes durante su distribución fuera de los locales del responsable? ¿Y para los dispositivos portátiles?
- ¿Se conservan las copias de respaldo y los procedimientos de recuperación de los datos personales en lugar diferente de aquel en que se encuentran los equipos informáticos que los tratan?
- ¿Se conserva, al menos durante dos años, un registro de los accesos que se realizan al sistema de información? ¿Permite dicha información identificar el registro accedido en caso de que el acceso se haya permitido?
- ¿Se han establecido procedimientos que impidan la desactivación de este registro de accesos?
- ¿Se han establecido procedimientos para que el responsable de seguridad revise al menos una vez al mes el registro de accesos?
- Si los datos se transmiten a través de redes públicas de telecomunicaciones o redes inalámbricas, ¿se procede al cifrado de los datos?

SEGURIDAD FICHEROS MANUALES

NIVEL BÁSICO

- ¿Se han definido criterios de archivo para garantizar la correcta conservación de los documentos, su localización, su consulta y el ejercicio de los derechos ARCO?
- ¿Los dispositivos de almacenamiento de documentos están dotados de mecanismos que dificulten su apertura?
- ¿Se ha informado y concienciado al personal que el deber de custodia de los documentos cuando estén fuera del archivo es de la persona que se encuentre a su cargo?
- ¿Se han definido claramente en el documento de seguridad las funciones y obligaciones de los usuarios que acceden a los sistemas de información que contienen datos personales?

- ¿Se ha creado un registro de incidencias y un procedimiento para su gestión? ¿Se ha difundido este procedimiento para conocimiento general de todo el personal?
- ¿Se ha asegurado que cada usuario acceda únicamente a los datos personales que son necesarios para sus funciones?
- ¿Existen medidas adecuadas para identificación, inventario, control de acceso y autorización de la salida de soportes?
- ¿Se han adoptado las medidas adecuadas para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

NIVEL MEDIO

- ¿Se ha designado un responsable o responsables de seguridad?
- ¿Se realizan auditorías bienales o cada vez que se produzcan modificaciones sustanciales en los sistemas de información?

NIVEL ALTO

- ¿Se conservan los armarios y archivadores en áreas separadas protegidos con puertas de acceso con llave u otro dispositivo equivalente?
- ¿Se mantienen cerradas salvo cuando accede al área el personal autorizado en el DS?
- ¿La generación de copias o la reproducción de documentos se lleva a cabo bajo el control del personal autorizado en el DS?
- Una vez que no son necesarias, ¿se procede a la destrucción de copias de manera que se evite el acceso a los datos personales contenidos en las mismas?
- ¿Se ha establecido un mecanismo de registro e identificación de los accesos a la documentación? ¿Y un procedimiento para registrar accesos de personal no autorizado?
- ¿Se adoptan medidas para impedir el acceso o la manipulación de la información durante su traslado?

16. ANEXO II. DOCUMENTOS MODELO

Como posibles ejemplos de tablas que pueden utilizarse para sistematizar la información sobre flujos de información e identificación y gestión de riesgos, se incluyen los siguientes modelos.

MODELO PARA DESCRIPCIÓN DE FLUJOS DE INFORMACIÓN

Código de identificación	Descripción	Origen de la información	Destinatarios de la información	Categorías de datos	Finalidad	Causa legitimadora
1						
2						
3						
…						

MODELO PARA GESTIÓN DE RIESGOS

Código de identificación del riesgo	Descripción del riesgo	Nivel de impacto si el riesgo se materializa	Probabilidad de que se materialice	Medidas propuestas	Impacto tras implantación de medidas propuestas	Probabilidad tras implantación medidas propuestas
1						
2						
3						
…						

NIVELES DE IMPACTO EN LOS DERECHOS FUNDAMENTALES DE LOS AFECTADOS Y EN LA ORGANIZACIÓN

- Muy alto
- Alto
- Medio
- Bajo
- Muy bajo

También se puede optar por una escala numérica a elección del responsable (por ejemplo, entre 0 y 10).

PROBABILIDAD DE MATERIALIZACIÓN DEL RIESGO

- Muy alta (81%-100%)
- Alta (61%-80%)
- Media (41%-60%)
- Baja (21%-40%)
- Muy baja (0%-20%)

17. ANEXO III. MODELO DE INFORME FINAL DE UNA EIPD

[1] Identificación del proyecto

I. Código

II. Descripción

III. Responsable(s) del proyecto y datos de contacto

IV. Fecha del informe

V. Versión del informe

[2] Resumen ejecutivo

I. Descripción sucinta del proyecto

II. Principales riesgos identificados

III. Resumen de las medidas más importantes de mitigación propuestas

[3] Análisis de necesidad de la Evaluación

I. Resultado del análisis

II. Motivación de la necesidad de la realización de la EIPD

[4] Descripción detallada del proyecto

I. Inclusión de toda la información relevante sobre el mismo (se pueden incluir como anexos los documentos del proyecto que se juzguen oportunos)

II. Descripción detallada de los flujos de datos personales

[5] Resultado del proceso de consultas

I. Identificación de las partes interesadas (internas y externas) o a las que afecta el proyecto

II. Contribuciones de las partes consultadas (se pueden incluir como anexos al informe)

III. Resumen de los riesgos más importantes puestos de manifiesto en la consulta

[6] Identificación y gestión de riesgos

I. Identificación detallada de riesgos

II. Impacto y probabilidad de cada riesgo identificado

III. Gestión de los riesgos: decisión adoptada para cada riesgo, objetivos de control, controles y medidas propuestas

[7] Análisis de cumplimiento normativo

I. Resumen general de cumplimiento

II. Deficiencias detectadas y propuestas de solución

[8] Conclusiones

I. Análisis final

II. Recomendaciones del equipo responsable de la EIPD

III. Medidas técnicas que deben adoptarse en el diseño del proyecto para eliminar o evitar, mitigar, transferir o aceptar los riesgos para la privacidad

IV. Medidas organizativas que deben adoptarse en el diseño del proyecto para eliminar o evitar, mitigar, transferir o aceptar los riesgos para la privacidad

[9] Anexo. Introducción y descripción general del proceso de evaluación

18. ANEXO IV. GLOSARIO

Big data. Cantidades masivas de datos que se recogen a lo largo del tiempo y que no se pueden analizar con las herramientas de bases de datos tradicionales. Para su tratamiento se utilizan ordenadores de gran potencia y programas de inteligencia artificial. Los datos tratados en este ámbito incluyen transacciones comerciales, textos no estructurados publicados en la web (por ejemplo, en blogs y redes sociales), mensajes de correo electrónico, fotografías, vídeos (en particular, vídeos de vigilancia), ingentes cantidades de datos de múltiples sensores y *logs* de actividad. Su objetivo es analizar dichos datos para establecer correlaciones entre ellos con las más diversas finalidades: segmentación de mercados, construcción de perfiles de consumidores, análisis de riesgos, lucha contra el fraude, análisis de mercados financieros, etc.

Ciudades inteligentes (Smart cities). Una ciudad inteligente es aquellas que utiliza las TIC para conseguir un crecimiento económico sostenible, un uso adecuado de los recursos naturales y una mayor calidad de vida para sus ciudadanos así como para fomentar la participación de los mismos en el gobierno de la ciudad.

Cloud computing (Computación en la nube). Conjunto de servicios basados en la web en los que los usuarios disponen de una gran variedad de capacidades funcionales por las que pagan solo en la medida que las usan. Es un modelo de computación que se basa en la compartición de recursos en la red en lugar de utilizar servidores locales o propietarios de cada organización.

Cookies. Fichero de texto que los navegadores almacenan en los ordenadores de los usuarios y que, posteriormente, pueden ser actualizados y recuperados por la entidad responsable de su instalación con diversas finalidades. Entre ellas destaca la posibilidad de realizar un seguimiento y monitorización de la navegación del usuario en internet.

Data Loss Prevention. Producto diseñado para detectar potenciales filtraciones o accesos no autorizados a los datos de un sistema de información. Se basa en la monitorización, detección y

bloqueo de la utilización de dichos datos ante una actividad sospechosa tanto cuando están en reposo como cuando se utilizan o se transmiten.

Drones. Vehículos aéreos no tripulados guiados por control remoto.

Intrusion Detection System (IDS). Sistema diseñado para monitorizar el tráfico entrante y saliente en un sistema informático para identificar patrones sospechosos que pudieran indicar la posibilidad de un ataque malicioso.

Intrusion Prevention System (IPS). Herramienta por la que se pueden definir reglas y procedimientos para alertar sobre tráfico sospechoso en un sistema o red informática y, basándose en las mismas, permitir a los administradores de sistemas definir acciones que se ejecutarán tras la alerta.

Inteligencia Artificial. Ciencia que trata de la reproducción de las características de la inteligencia humana en los ordenadores. También se puede definir como el estudio y diseño de agentes inteligentes (sistemas que perciben el entorno y toman decisiones que maximizan sus probabilidades de éxito).

Internet de las cosas (Internet of things). Red de dispositivos interconectados a través de internet que se comunican entre ellos y que pueden realizar acciones en función del entorno y las informaciones que reciben.

Logging. Registro de las actividades de un sistema de información y de las acciones que los usuarios realizan en él. Puede utilizarse para detectar debilidades de seguridad y comportamientos ilícitos de los usuarios.

Metadatos. Literalmente, significa «datos sobre los datos», es decir, son datos que describen otros datos y que permiten que los mismos sean localizados y procesados más fácilmente. Por ejemplo, cuando se produce una llamada telefónica, la hora, el número de origen, el número de destino y la duración de la misma son metadatos relativos a dicha llamada telefónica y que pueden ayudar a su localización o selección.

Minería de datos (Data Mining). Es un proceso computacional para el descubrimiento de patrones comunes y la extracción de información y conocimiento analizando grandes volúmenes de datos con técnicas de inteligencia artificial.

Need to know (Necesidad de conocer). Se refiere a la técnica de control de acceso a la información mediante la cual se garantiza que una persona o recurso solo accede a aquellos datos que le resultan estrictamente necesarios para realizar sus funciones. Su objetivo es dificultar el acceso

no autorizado a la información limitando al mínimo imprescindible las personas que tienen acceso a la misma.

Privacy by Design (Privacidad desde el diseño). Aproximación al diseño de sistemas de información que tiene en cuenta los requisitos de privacidad desde las etapas iniciales del mismo y a lo largo de todo su ciclo de vida. El concepto fue acuñado en 1995 en un informe conjunto de las autoridades de protección de datos de los Países Bajos y Ontario (Canadá) titulado *Privacy-enhancing technologies.*

Privacy Impact Assessment (PIA). Revisión sistemática de un producto, servicio o sistema de información para identificar los riesgos que puede suponer para la privacidad e implantar las medidas necesarias para eliminarlos o mitigarlos hasta niveles aceptables.

RFID (Radio-frecuency Identification). Uso de los campos de frecuencia electromagnética para transmitir datos de forma inalámbrica desde etiquetas RFID a lectores electromagnéticos que los transfieren a un ordenador para la identificación y seguimiento de los objetos a los que se unen dichas etiquetas. Al contrario que los códigos de barras, esta tecnología permite leer una etiqueta que no esté en el *campo de visión* del lector.

www.agpd.es