MODELO DE INFORME DE EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS (EIPD) PARA EL SECTOR PRIVADO

Este modelo de informe está orientado a ayudar a los responsables a cumplir con las previsiones del Reglamento General de Protección de Datos cuando sea necesario realizar una Evaluación de Impacto para la Protección de Datos, dentro del marco de la gestión del riesgo para los derechos y libertades de las personas.

Teniendo en cuenta que este informe es en sí mismo una herramienta de trabajo, el lenguaje utilizado deberá ser lo suficientemente claro y explicativo, y ha de adaptarse a la audiencia a la que se orienta, por lo que podría existir distintas versiones de éste. Los receptores del informe puede que sean personas que jurídica o técnicamente no se encuentren habituadas a la terminología de protección de datos personales. Especial relevancia tendrá el lenguaje utilizado cuando el informe se destine a los gestores que, en base al mismo, tengan que aprobar y aplicar la EIPD y, en consecuencia, tomar decisiones relacionadas con el tratamiento o tratamientos de datos personales objeto de la EIPD, decisiones que afectarán a los derechos y libertades de las personas físicas cuyos datos vayan a ser tratados.

Este modelo contiene los capítulos y apartados mínimos que han de aparecer en la documentación de una EIPD. Dependiendo de su complejidad, el contenido de la EIPD podría ser un único documento o distribuirse en varios.

La EIPD es un proceso dentro del marco de la gestión del riesgo. Por lo tanto, cumplimentar el presente modelo no debe de entenderse como la EIPD sino que viene a resumir las actuaciones que el responsable hubiera realizado siguiendo las recomendaciones que se señalan en la Guía práctica para la Gestión del riesgo y evaluación de impacto en tratamientos de datos personales sujetas al RGPD de la AEPD (en adelante la Guía) y, de este modo, dando respuesta a los requisitos mínimos que la Instrucción 1/2021 de la AEPD (en adelante la Instrucción) exige para llevar a cabo, en caso necesario, una posible solicitud de consulta previa a la Autoridad de Control en los casos en los que así lo requiere el artículo 36.1 y, como se señala en el considerando 94 del RGPD, cuando el responsable del tratamiento considere que el riesgo no puede mitigarse por medios razonables.

Por otra parte, a fin de poder comprobar que la EIPD se ajusta a los requisitos formales mínimos señalados en la Instrucción deberá utilizarse la lista de verificación (en adelante “la Lista”).

NOTA: Estos cuadros tienen el propósito de incluir una descripción de cada apartado del documento. No reemplazan a las Guías citadas y deberán eliminarse del informe final.

I. RESUMEN EJECUTIVO

En este apartado se deberán señalar los objetivos que se persiguen con la EIPD reflejando, de forma condensada, los aspectos más significativos de los capítulos que se desarrollan a lo largo de todo el documento. En ningún caso, los objetivos de una EIPD, deberán entenderse de forma exclusiva en términos de cumplimiento sino en términos de gestión del riesgo para la protección de los derechos y libertades de las personas físicas.

Este resumen contendrá la denominación del tratamiento y su versión, la identificación del responsable del tratamiento, de la unidad responsable en la organización, unidades gestoras de los datos que intervienen en alguna de las fases del tratamiento, encargados y subencargados del tratamiento y cesiones de datos previstas.

A su vez, incluirá una breve descripción del tratamiento, su finalidad, las principales categorías de datos, operaciones de tratamiento significativas y su planeada implementación, así como las conclusiones del análisis de necesidad, idoneidad y proporcionalidad del tratamiento y de las bases jurídicas que legitiman el tratamiento de los datos.

Finalmente, incluirá una breve descripción sobre el contexto de la EIPD y del proceso de gestión formal de los riesgos entre los que se incluirá una breve referencia a la metodología utilizada, la extensión y límites de la EIPD, los riesgos de privacidad identificados más significativos, las soluciones de gestión y técnicas planeadas, una síntesis del análisis del coste en privacidad con relación al beneficio para los sujetos de los datos y las conclusiones derivadas del riesgo residual y, en particular, la necesidad de realizar o no realizar una consulta previa a la AEPD.

II. INDICE

III. DATOS BÁSICOS

A. Identificación del Responsable-RGPD

Identificación de la Entidad Responsable-RGPD, y si procede identificación de corresponsables, así como del resto de intervinientes e implicados en el tratamiento con la definición inequívoca de sus obligaciones y tareas.

Identificación del representante del responsable en caso de que el responsable esté fuera de la Unión Europea.

Identificación de un punto de contacto (POC) en la Entidad Responsable/corresponsable (si cabe DPD) así como cada uno de los responsables o POC de cada una de las unidades gestoras o unidades funcionales que intervienen en el tratamiento. En su caso, incluir fecha de notificación del DPD a la AEPD.

Detalles de la implicación del DPD en la EIPD en términos de asesoramiento, supervisión y ejecución.

Identificación de la unidad o unidades gestoras a cargo de la gestión del tratamiento dentro de la organización Responsable.

B. Nombre y descripción del tratamiento

Nombre interno dado al tratamiento, denominación del mismo en el Registro de Actividades de Tratamiento, y, si cabe, identificación de la versión del tratamiento con indicación del historial de cambios y modificaciones realizadas sobre el tratamiento, si las hubiera, en cada una de las etapas del mismo.

Breve descripción del tratamiento, incluyendo la información establecida en el artículo 31 de la LOPDGDD (30 del RGPD) con relación al registro de actividades de tratamiento.

Para la administración pública aquí tendríamos que poner lo del artículo 77 de LOPDGDD y el inventario de tratamiento.

C. Fecha prevista de inicio del tratamiento

Incluirá las fechas estimadas en las que se prevé iniciar el tratamiento.

En caso de que el tratamiento se haya iniciado con anterioridad a la EIPD y/o a la consulta previa y se estime necesaria la consulta previa, se incluirá una justificación objetivamente motivada acerca de las razones por las que inicialmente no fue necesaria la EIPD o la consulta previa y de las razones por las que posteriormente se estimaron necesarias, de acuerdo con el apartado X.C de la GUÍA.

D. Fecha de fin del tratamiento o condiciones de caducidad

Se incluirá la fecha en la que se prevé finalizar el tratamiento y/o las condiciones de caducidad del mismo.

IV. METODOLOGÍA DE LA EIPD

A. Implicados en la ejecución de la EIPD

De forma breve, se describirá el equipo de trabajo que ha realizado este informe y está implicado en la gestión del riesgo para los derechos y libertades, detallando sus roles, tareas, responsabilidades, etc. En este apartado podrá hacerse uso de una matriz RACI.

Si se ha recabado la opinión de los interesados o de sus representantes en el proceso de identificación y evaluación del riesgo para los derechos y libertades se deberá incluir describir su implicación en el proceso de la EIPD en línea con el capítulo XV de la GUÍA.

B. Guías, herramientas, metodologías y normas utilizadas en la evaluación

Se detallarán las directrices, normas, guías y otro material de referencia utilizado en la realización de la EIPD. En particular se detallará su adecuación a lo establecido en la Instrucción 1/2021 con relación a las Consultas Previas.

C. Extensión y límites de la EIPD: Identificar que ha quedado fuera de la evaluación

Se deberán indicar los motivos por los que se limita el alcance de la EIPD con relación a los fines, el ámbito o alcance del tratamiento, incluyendo aquellos aspectos que quedarían fuera de su análisis y los posibles riesgos asociados para los derechos y libertades de las personas, incluyendo la forma en la que podrían ser abordados y la identificación de los responsables de dichos riesgos.

D. Fecha de realización del informe de la EIPD

Fecha, hora e identificación de quien coordina el equipo que lleva a cabo la EIPD sobre la realización del presente informe.

Versión o revisión de la realización del informe EIPD y firma del responsable.

Histórico de cambios y modificaciones, en general cualquier elemento que pueda demostrar el seguimiento llevado a cabo por el responsable.

V. ANÁLISIS DE BASES JURÍDICAS DEL TRATAMIENTO Y CUMPLIMIENTO NORMATIVO

En este capítulo se desarrolla la base jurídica y, en su caso, normas y/o supuestos habilitantes que justifican el tratamiento que se pretende llevar a cabo.

Hay que ser conscientes que el cumplimiento normativo no entra a formar parte del análisis de riesgos, sino que el cumplimiento de principios y deberes es preceptivo.

La ausencia de una base jurídica para el tratamiento, o la existencia de dudas sobre dicha base jurídica, no puede sustituirse con la adopción de garantías derivadas de una gestión del riesgo para los derechos y libertades de los ciudadanos.

En ningún caso, la justificación de la adopción de una base jurídica es el objeto de este documento.

El análisis de las bases jurídicas se realizará con relación a cada uno de los fines del tratamiento incluyendo fines secundarios o ulteriores.

La licitud de las bases jurídicas tendrá que justificarse según las condiciones que se cumplan de acuerdo con el artículo 6 del RGPD.

En el caso de que se traten categorías especiales de datos (Artículo 9 RGPD y Artículo 9 LOPD) se deberá señalar justificadamente los motivos que dieron lugar al levantamiento de la prohibición de tratar categorías especiales de datos. Si el levantamiento de la prohibición se lleva a cabo mediante el consentimiento se habrán analizado las condiciones de dicho consentimiento.

Para completar este apartado se recomienda consultar la Lista de Cumplimiento Normativo publicada por la AEPD en su página web.

VI. DESCRIPCIÓN DEL TRATAMIENTO

Una correcta gestión del riesgo para los derechos y libertades exige conocer los detalles del tratamiento lo que implica la necesaria descripción sistemática del tratamiento.

La mejor forma de realizar la descripción de un tratamiento es la que se ajuste a la descripción de procesos que ya se utilicen en los sistemas de gestión y de calidad de la entidad. La granularidad que se debe alcanzar en la descripción del tratamiento ha de ser la suficiente para que sea posible realizar dicha gestión. En este sentido se podría estudiar el tratamiento en varios niveles de detalle, por ejemplo:

• Estudio a alto nivel del tratamiento.

• Análisis estructurado del tratamiento, o descomposición del tratamiento en fases para realizar el estudio individual de las mismas.

• Análisis del ciclo de vida de los datos.

Finalmente, a partir del análisis estructurado del tratamiento será posible obtener el Inventario de activos asociado a un tratamiento atendiendo a los diferentes casos de uso a los que el diseño del mismo debe dar respuesta.

La descripción del tratamiento, con independencia del método utilizado, al menos deberá incluir:

• El tipo de acuerdo o acto jurídico entre corresponsables implicados o terceros que intervienen en el tratamiento, así como el acto jurídico que les vincula con el tratamiento y legitima su participación en el mismo y si dicho vínculo especifica y define las medidas y garantías de responsabilidad proactiva que han de implementar el encargado y subencargados

• La existencia de garantías jurídicas para garantizar la consulta al responsable por parte de encargados antes de abordar la contratación.

• Las medidas previstas para garantizar y demostrar el cumplimiento de las previsiones del RGPD y la LOPDGDD, teniendo en cuenta las obligaciones de información a los interesados, los procedimientos para garantizar los derechos de los interesados.

• Las cesiones de datos previstas y las transferencias internacionales de datos.

• Los códigos de conducta, sellos, marcas y certificaciones aplicables en cada caso.

Etc.

A. Estudio a alto nivel del tratamiento

Si la descripción del tratamiento se realiza mediante un estudio a alto nivel del mismo, en este apartado se deberán incluir todos los aspectos relevantes del análisis del tratamiento de una manera conjunta.

Al menos, el estudio a alto nivel del tratamiento deberá incluir la información que se señala en el apartado V.A de la GUÍA con relación a la naturaleza, los fines, el alcance y el ámbito, y el contexto del tratamiento

B. Análisis estructurado del tratamiento

Si la descripción del tratamiento exige un mayor grado de detalle podrá realizarse mediante un análisis estructurado del tratamiento. En este apartado se incluirá la

información del estudio a alto nivel del tratamiento y se identificarán las distintas operaciones de tratamiento que se lleven a cabo además del detalle de la relación existente entre las mismas teniendo en cuenta la naturaleza, los fines, el alcance y el ámbito, y el contexto del tratamiento. El grado de descripción de cada operación tendría que ser acorde al impacto en el riesgo que podría tener dicha fase.

Se puede encontrar más detalle de cómo plantear el análisis estructurado en el apartado V.B de la GUÍA.

C. Descripción del ciclo de vida de los datos

Finalmente, si para realizar la descripción sistemática del tratamiento se requiere un nivel de detalle mayor, es recomendable realizar un análisis global del ciclo de vida de los datos en el que se partirá del análisis a alto nivel y del análisis estructurado del mismo.

El análisis del ciclo de vida supone estudiar, para un conjunto o categoría de datos, las distintas etapas de su vida, desde su recogida o generación hasta su destrucción. La descripción del ciclo de vida de los datos es un análisis complementario al análisis a alto nivel y al análisis estructurado del tratamiento.

En el apartado V.C de la GUÍA se puede encontrar información más detallada al respecto.

Asimismo, se aportará una descripción de las cesiones y destinatarios de las mismas, con relación a los fines, al ciclo de vida del tratamiento, al ciclo de vida del dato y las operaciones de tratamiento además de la descripción funcional en la que se llevan a cabo dichas cesiones para cada uno de los destinatarios. Se vincularán las cesiones de datos con las bases jurídicas que las legitiman.

D. Inventario de activos

Partiendo del resultado del análisis estructurado o de la descripción del ciclo de vida de los datos en el tratamiento, será posible obtener la relación de todos los activos necesarios para abordar el inicio del tratamiento y una adecuada gestión de los riesgos para los derechos y libertades de las personas físicas.

Los activos deberán incluirse, organizarse y mantenerse actualizados, en lo que se denomina el inventario de activos del tratamiento. Activo se define como todo bien o recurso que puede ser necesario para implantar y mantener una operación de tratamiento en cualquier etapa de su ciclo de vida, desde su concepción y diseño hasta la retirada del tratamiento.

El nivel de detalle a incluir en el inventario de activos debería ser el necesario para identificar y gestionar el riesgo de manera eficiente y, al mismo tiempo, poder demostrar dicha gestión.

El inventario de activos se debe determinar a partir del análisis estructurado del tratamiento, o mediante cualquier otro procedimiento determinado por la entidad, de igual o mayor eficacia.

No disponer de un adecuado inventario de activos actualizado, puede implicar la toma de decisiones inadecuadas con relación al tratamiento y, en el caso de llevar a cabo una consulta previa, la Autoridad de Control podrá concluir que la información proporcionada es incompleta, incorrecta y, por tanto, inexacta, sin perjuicio del quebrantamiento de otros principios como el de transparencia.

En el apartado V.D de la GUÍA se describe la información necesaria para documentar los activos del tratamiento.

E. Casos de uso

Atendiendo a la complejidad del tratamiento, pueden existir diferentes casos de uso del mismo a fin de dar respuesta a diferentes procesos de una organización, en la descripción del tratamiento en sus distintos niveles de detalle, se deberá identificar a qué caso de uso se refiere y marcar sus diferencias.

Asimismo, se deberán identificar y documentar las medidas de privacidad por defecto y se ha planificado su implementación para cada caso de uso.

La identificación de casos de uso, con ejemplos, se ha tratado en la Guía de Protección de Datos por Defecto. Y también se encuentra disponible online el Listado de medidas de Protección de Datos por Defecto.

VII. IDENTIFICACIÓN Y ANÁLISIS DE LOS FACTORES DE RIESGO

La identificación y el análisis de los factores de riesgo para los derechos y libertades de las personas físicas es el paso previo a la evaluación del nivel de riesgo inherente del tratamiento.

En el contexto de la responsabilidad activa, la identificación y análisis de factores de riesgo estará siempre documentada y justificada a fin de que el responsable pueda demostrar que, las decisiones tomadas en cada momento con relación a la gestión del riesgo han sido las medidas más adecuadas en función de la información de la que se disponía ("*accountability*").

Con el objeto de apoyar la realización de esta tarea, la AEPD pone a disposición de los responsables y encargados del tratamiento la herramienta EVALÚA_RIESGO RGPD que tiene como objeto servir de ayuda a responsables y encargados a identificar los factores de riesgo para los derechos y libertades de los interesados presentes en el tratamiento, haciendo una primera evaluación del riesgo intrínseco, ayudando a determinar obligación de realizar una EIPD, a la vez que puede también servir en el proceso de gestión del riesgo residual del tratamiento.

En ningún caso EVALÚA_RIESGO RGPD representa la totalidad de los factores de riesgo de todo el conjunto posible de tratamientos sino una base y metodología para la identificación de los posibles factores de riesgo inherente de un tratamiento y no una lista cerrada de factores de riesgo. Corresponde al responsable identificar el conjunto de los posibles factores de riesgo que pudieran afectar al tratamiento de datos personales que se pretende llevar a cabo en cada caso.

A. Identificación de los factores de riesgo

En la gestión del riesgo y durante la fase de análisis, además de los que se contemplan en el RGPD, y en su desarrollo a través de la LOPDGDD, normativa especial, y listas, guías y directrices aprobadas por las autoridades de protección de datos, donde se identifican un conjunto de factores de riesgo, también se deben identificar y evaluar aquellos factores de riesgo que derivan del tratamiento concreto en función de su naturaleza, ámbito o extensión o los fines que persigue, sin olvidar, tampoco, aquellas otras que se derivan del contexto presente (interno y externo a la organización) y futuro del tratamiento.

En los apartados VI.C y VI.E de la GUÍA se desarrollan en detalle una serie de listados de factores de riesgo identificados en la normativa.

B. Análisis de los factores de riesgo

Para cada uno de los factores de riesgo identificados, el responsable deberá determinar el impacto inherente, es decir, aquel que resulta de no considerar las medidas y garantías para los derechos y libertades. El impacto dependerá del daño que se pueda ocasionar a los interesados en particular y a la sociedad en su conjunto, en el ámbito de sus derechos y libertades, a corto, medio y a largo plazo.

A su vez, también será necesario determinar la probabilidad de que el riesgo identificado se materialice.

Si bien se puede hacer el análisis conforme a cualquier metodología reconocida, en el apartado VI.B de la GUÍA se dan una serie de indicaciones de cómo se puede realizar

este análisis de los factores de riesgo a fin de dar cumplimiento a lo exigido en la Instrucción.

C. Análisis de los escenarios de brechas de datos personales

En la práctica, el proceso de evaluación del nivel de riesgo no puede llevarse a cabo sin tener en cuenta las posibles consecuencias de las brechas de datos personales sobre los interesados con el fin de establecer criterios de coherencia en la evaluación del riesgo impidiendo que la evaluación inicial del riesgo pueda diferir con relación a las consecuencias sobre los interesados resultante de la pérdida de confidencialidad, integridad, disponibilidad de los datos, reversión de la anonimización/seudonimización, uso de los datos para fines no compatibles, incumplimiento de garantías, etc.

Por ello, en la identificación y análisis de factores de riesgo, es necesario determinar los perjuicios que puede tener la materialización de brechas de datos personales en sus distintas dimensiones.

En el apartado VI.D de la GUÍA se incluye una orientación detallada para el análisis de estos perjuicios en caso de que se produzcan brechas de datos personales.

D. Evaluación del riesgo intrínseco

Es necesario realizar un análisis del riesgo intrínseco total del tratamiento, de acuerdo con el artículo 35.7.c del RGPD, teniendo en cuenta los elementos identificados a partir del resultado de la evaluación del nivel de riesgo para cada uno de los factores de riesgo identificados en el tratamiento.

La interdependencia de los distintos factores de riesgo podría elevar el nivel de riesgo del tratamiento por encima del peor caso de cada factor de riesgo tomado individualmente. Cuando hay distintos factores de riesgo es necesario interpretar cómo dichos factores, considerados de forma independiente, podrían interactuar entre sí para incrementar el nivel de riesgo del tratamiento (factor de riesgo acumulado), mediante el análisis de sus dependencias y efectos combinados o las interacciones mutuas que existan entre ellos.

En el capítulo VII de la GUÍA se da una orientación más detallada de esta evaluación.

VIII. ANÁLISIS DE LA OBLIGACIÓN Y ANÁLISIS DE NECESIDAD DE REALIZAR UNA EIPD

A. Inclusión del tratamiento en la lista de tratamientos exentos

Si el tratamiento está en la lista de tratamientos exentos establecida en el marco del artículo 35.5 del RGPD, no es obligatorio realizar la EIPD, y el informe terminaría aquí, a menos que a continuación se motiven las razones por las que el responsable ha tomado la decisión de llevar a cabo la evaluación de impacto (ver apartados XI y XII de la GUÍA).

Dicha lista, aprobada por el Comité Europeo de Protección de Datos, puede consultarse aquí y su carácter es meramente orientativo.

B. Análisis de la inclusión del tratamiento en los casos de tratamientos obligados

En este apartado se determinará si hay obligación de realizar la EIPD. Para ello se tendrá en cuenta, en particular, si el tratamiento:

- Entra en la lista de casos enumerados en el artículo 35.3 del RGPD.
- Cumple con las condiciones que se detallan en la lista, aprobada por el Comité Europeo de Protección de Datos, de tratamientos obligados (artículo 35.4 del RGPD) que puede consultarse aquí y su carácter es meramente orientativo.
- Se dan los supuestos de mayor riesgo de los casos enumerados en el artículo 28.2 de la LOPDGDD.

Se recomienda hacer uso de la herramienta Evalúa-Riesgo RGPD para el análisis de los factores de riesgo inherentes al tratamiento que se plantea en la EIPD.

Con independencia de todo lo señalado, el responsable podría asumir necesaria la realización de la EIPD, en tal caso, deberán señalarse los posibles motivos que a juicio del responsable hicieran necesaria la EIPD (políticas de protección de datos, requisitos de calidad, etc.).

IX. CONTROLES PARA LA REDUCCIÓN DEL RIESGO

El objeto de este apartado es el de establecer medidas de gestión, organización, definición del tratamiento, procedimentales y técnicas que permitan gestionar cada uno de los elementos de riesgo identificados en el apartado VII "Análisis de la obligación de realizar una EIPD: evaluación del riesgo"

Se puede consultar información más detallada en el capítulo VIII de la GUÍA.

A. Medidas sobre el concepto y diseño del tratamiento

Estás medidas actuarán en la propia definición de la naturaleza, ámbito, contexto o fines del tratamiento, es decir, la esencia del tratamiento tal y como está concebido y diseñado.

Sobre la descripción original del tratamiento se ha de optimizar, desde el punto de vista de protección de datos, la descomposición de este en fases o subprocesos, para poder aplicar con más granularidad las medidas de reducción del riesgo.

De esta forma, también identificar posibles fases innecesarias, aislar las de mayor nivel de riesgo del resto de fases, determinar medidas específicas para gestionar las fases de mayor riesgo y determinar aquellas que no precisan de acceso a datos personales.

Entre las posibles medidas o garantías que se podrían adoptar estarían las recogidas en el apartado VIII.A de la GUÍA. También, para una mayor orientación sobre este apartado se aconseja consulta la Guía de Protección de Datos por Defecto publicada por AEPD.

B. Medidas de gobernanza y las políticas de protección de datos

En este apartado se señalarán las medidas de gobernanza y las políticas de protección de datos de la entidad (*accountability)* son todas aquellas dirigidas a implementar un sistema de gobernanza de los datos personales que permitan demostrar el cumplimiento de:

-Principios

-Derechos

-Garantías para gestionar el riesgo.

En particular:

- Medidas que permitan tener un control sobre qué datos se acceden, por quién, de quien, cuando, con qué legitimación y propósito, que tratamientos se han realizado sobre ellos

- Medidas para asegurar que los sistemas de gestión de derechos se ejecutan de forma adecuada

- Medidas para conservar la trazabilidad de los datos comunicados a terceros

- Nombramiento de DPD

- Medidas para notificar a los sujetos de los datos incidentes de seguridad que afecten a sus derechos y libertades

- Intervención humana por parte del responsable en los tratamientos que impliquen decisiones individuales automatizadas

- etc.

En el apartado VIII.B de la GUÍA se puede consultar un listado mucho más exhaustivo de ejemplos de posibles medidas de gobernanza y políticas de protección de datos.

C. Medidas de protección de datos desde el Diseño

Las medidas de Privacidad desde el Diseño y por Defecto aplicables dependerán del tipo de tratamiento. Además, se aplicarán medidas específicas en las distintas fases del tratamiento, por lo tanto, la aplicación de estas medidas está relacionada con el apartado anterior de Optimización del Tratamiento.

Para resolver este apartado se aconseja consultar, en particular, la Guía de privacidad desde el Diseño publicada por la AEPD, y en general, las guías y notas publicadas en la web de la AEPD en el apartado Innovación y tecnología.

Una lista, para tratamientos genéricos y no exhaustiva, se deriva de lo establecido en el artículo 25 del RGPD, y son medidas que abarcan la minimización, la ocultación, la separación, la abstracción, la información, el control, el cumplimiento y la demostración, que pueden encontrarse de forma resumida en el apartado VIII.C de la GUÍA.

D. Medidas de Seguridad y de gestión de brechas de datos personales

En este apartado se detalla el análisis de los requisitos necesarios para minimizar riesgos para los derechos y libertades sobre los dominios de seguridad: confidencialidad, disponibilidad, e integridad y como se realiza la integración de dichos requisitos con el resto de los requisitos de seguridad (para continuidad de negocio, control de fraude, etc.) de la organización.

Además, se incluirá específicamente la gestión de la entidad en el caso de que se produzcan brechas de datos personales.

Puede ser conveniente anexar al documento la relación de medidas aplicables firmada por el responsable de seguridad.

En el apartado VIII.D de la GUÍA se puede consultar una orientación detallada de las medidas de seguridad aplicables para la protección de derechos y libertades.

E. Reevaluación del riesgo

La gestión del riesgo es un proceso iterativo, la aplicación de una medida para paliar o mitigar un riesgo puede, a su vez, ocasionar la aparición de nuevos riesgos o consecuencias no deseadas para los interesados. Deberá de realizarse nuevamente, tras la aplicación de las medidas, una reidentificación y evaluación de riesgos.

El riesgo residual deberá cuantificarse de acuerdo con la política de gestión del riesgo de la organización.

La GUÍA recoge en su capítulo IX orientación sobre esta reevaluación necesaria en la evaluación de impacto.

F. Plan de acción de la gestión de riesgos

En este apartado se detallarán las acciones necesarias para llevar a cabo la adecuada gestión del riesgo para los derechos y libertades de las personas, reflejando el conjunto de acciones necesarias para la revisión y actualización de las medidas que hubieran sido identificadas en la EIPD.

El plan de acción puede venir definido mediante las políticas de protección de datos (Artículo 24 del RGPD) que el responsable considere necesarias, incluyendo en las mismas, las cláusulas de caducidad del tratamiento.

En el mismo se ha de detallar los objetivos, tareas, calendario, los recursos necesarios, los responsables, así como la interacción con otros tratamientos de la organización.

En particular, tienen que quedar reflejadas las medidas de privacidad desde el diseño y por defecto que se hubieran definido en la EIPD para que la protección de datos sea una integral al producto/servicio, no una capa añadida.

X. ANÁLISIS DE LA NECESIDAD Y PROPORCIONALIDAD DEL TRATAMIENTO

Una de las exigencias del artículo 35 del RGPD con relación a la EIPD, es la que aparece en el apartado 35.7.b del RGPD, la obligación de que se realice "una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento en cuanto a su finalidad", análisis de necesidad y proporcionalidad que no debe de confundirse con el análisis de obligación o necesidad de llevar a cabo la EIPD.

La palabra "evaluar" implica la realización de un análisis objetivo que sustente una conclusión, por lo que no se reduce a una simple afirmación.

Este principio de proporcionalidad, llevado a la evaluación de la necesidad y proporcionalidad del tratamiento, se traduce en realizar una ponderación atendiendo a tres criterios:

- Juicio de idoneidad: Hay que determinar si el tratamiento es adecuado para el fin que persigue. El tratamiento da respuesta a determinadas carencias, demandas, exigencias, obligaciones u oportunidades objetivas y puede conseguir los objetivos propuestos con la eficacia suficiente.
- Juicio de necesidad: Hay que determinar si la finalidad perseguida no puede alcanzarse de otro modo menos lesivo o invasivo, es decir, no existe un tratamiento alternativo que sea igualmente eficaz para el logro de la finalidad perseguida.
- Juicio de proporcionalidad en sentido estricto: La gravedad del riesgo para los derechos y libertades del tratamiento, y su intromisión en la privacidad, ha de ser adecuada al objetivo perseguido y proporcionada a la urgencia y gravedad de esta. Hay que ponderar el beneficio que el tratamiento, desde el punto de vista de la protección de datos, proporciona a la sociedad manteniendo un equilibrio con el impacto que representa sobre otros derechos fundamentales. Sin embargo, aunque pueda ceder parcialmente, en ningún caso, se puede asumir la negación absoluta del derecho a la protección de datos y vaciarle de su contenido esencial.

Esta evaluación ha de terminar con una decisión de llevar o no a cabo el tratamiento, o en su caso, modificarlo para que cumpla con los tres juicios exigidos. En ningún caso se recomienda continuar con la EIPD cuando el tratamiento no supera la evaluación de la necesidad y/o la proporcionalidad.

El incumplimiento de estos requisitos no podrá abordarse o justificarse mediante formas alternativas de cumplimiento como, por ejemplo, las bases jurídicas o medidas técnicas y organizativas.

En el capítulo XIII de la GUÍA se recoge información detallada de cómo realizar estas evaluaciones.

A. Juicio de idoneidad

Se definirá el umbral de efectividad del tratamiento. Se establecerá de forma objetiva o cualitativa y basada en evidencias, determinando cuál es el umbral de efectividad que se debería alcanzar para cumplir con los fines del tratamiento.

Se evaluará la efectividad de la propuesta del tratamiento. Se valorará de forma objetiva, cualitativa y basada en evidencias, la efectividad del tratamiento, tal y como se ha planteado, verificando si da respuesta a las necesidades planteadas y con qué extensión.

B. Juicio de necesidad

Se determinará la relevancia de los fines del tratamiento. Se evaluará que los fines del tratamiento tienen la importancia suficiente para ser abordados con un tratamiento de alto riesgo.

Se verificará la adecuación de las operaciones del tratamiento, es decir, que cada una de ellas están orientadas a cumplir con los fines del tratamiento de una forma objetivamente demostrable.

Se justificará la configuración actual del tratamiento. Se evaluará que no existen otros tratamientos, que ya están en curso o que se podrían plantear, que resuelven los fines declarados sin incurrir en un alto riesgo, incluso aunque sea necesario introducir alguna modificación para cumplir los fines perseguidos.

Se indicarán las cláusulas de caducidad previstas en el tratamiento tanto por su naturaleza, como por su ámbito, su contexto y sus fines.

C. Juicio de proporcionalidad en sentido estricto

Se Identificará el grado de impacto del tratamiento en los derechos y libertades. Se requiere que se exprese, de forma detallada, las limitaciones o intrusiones a los derechos y libertades que puede suponer el tratamiento para el interesado. Esta evaluación es una tarea previa que ya se ha debido realizar en la determinación de los factores y niveles de riesgo analizados previamente, exponiendo en este punto de la evaluación sus conclusiones.

Se identificarán y describirán las medidas compensatorias. Se requiere detalle de los controles establecidos en el diseño del tratamiento para disminuir dicho impacto.

Se identificarán los beneficios del tratamiento. Se deben determinar las ventajas y beneficios que, de forma objetiva y con evidencias, tiene el tratamiento para los interesados, considerados de forma individual y como colectivo. Es decir, también ha de considerarse el beneficio social.

Se confirmará la existencia de identidad en la calidad de la información. S tiene que evaluar si existe simetría en la información analizada para el juicio de ponderación, es decir, si el nivel de análisis con relación al impacto es igual al nivel alcanzado en base a la información proporcionada respecto a las ventajas.

Se realizará un análisis BDB (Balance Daño-Beneficio). Se requiere una evaluación de si los beneficios para los interesados y la sociedad, previamente determinados, compensan y justifican el impacto para los derechos y libertades identificados en el primer punto de este juicio de proporcionalidad en sentido estricto.

XI. NECESIDAD DE CONSULTA PREVIA

En base a los resultados obtenidos, se describirá si es o no necesario realizar la consulta previa a AEPD.

En caso de que el riesgo residual sea bajo o escaso no tendrá lugar la posible consulta previa a la que refiere el artículo 36, si existieran riesgos para los que el responsable no hubiera podido adoptar medidas, deberá realizarse la debida solicitud de consulta previa a la que refiere el artículo 36 del RGPD atendiendo a los requisitos que señala la Instrucción. En este apartado se detallarán los riesgos para los que el responsable no ha podido adoptar medidas y que justifican la necesidad de llevar a cabo la solicitud de consulta previa.

En el caso de que se haya presentado con antelación una consulta previa sobre el mismo tratamiento, hay que detallar el conjunto de las modificaciones introducidas en la naturaleza, el contexto, el ámbito, los fines, los riesgos y las garantías en el tratamiento que pudieran hacer necesaria la EIPD y la consulta previa.

Si existen con antelación consultas previas realizadas a una Autoridad de Control, se incluirá una referencia expresa a la respuesta o respuestas de la Autoridad o Autoridades de Control.

La documentación aportada a la consulta previa deberá de garantizar que la información aportada es completa y exacta (Art. 36.3 RGPD), la consulta previa estará firmada por el responsable del tratamiento y remitida por el canal de consultas de la AEPD tal y como exige la Instrucción.

En el capítulo XVI de la GUÍA se puede encontrar más orientación al respecto.

XII. CONCLUSIONES Y RECOMENDACIONES

El equipo de trabajo que realice la EIPD reflejará, de forma sumaria, el resultado final de la gestión del riesgo para los derechos y libertades, las directrices generales para la implementación del tratamiento, se determina si el riesgo es lo suficientemente bajo y las siguientes acciones, en particular si procede la Consulta Previa a la AEPD de acuerdo con el artículo 36 del RGPD.

En definitiva, deberá señalarse al responsable la decisión del equipo que ha realizado la EIPD incluyendo los puntos de vista de sus integrantes.

XIII. MEMORANDO DEL DELEGADO DE PROTECCIÓN DE DATOS

A. Visión del DPD

Este apartado incluirá de forma condensada, el punto de vista del DPD con relación al tratamiento que se pretende realizar, demostrando su adecuada participación en el proceso de la EIPD desde la posición y funciones que exigen los artículos 38 y 39 del RGPD al responsable o responsables del tratamiento.

En general, el DPD deberá pronunciarse con relación a los posibles riesgos para los derechos y libertades de las personas físicas, a las potenciales consecuencias negativas que el tratamiento podría suponer para los interesados.

La opinión del DPD deberá incluir su visión de todo el proceso con relación a la potencial expectativa de confidencialidad de los interesados, evitando que los interesados puedan llevar a cabo malas interpretaciones con relación a potenciales injerencias en su vida personal y familiar.

B. Conclusiones y recomendaciones del DPD al responsable

De manera igualmente condensada o resumida, en este apartado se deberán incluir las conclusiones y recomendaciones que, en su labor de asesoramiento, el DPD realice al responsable o encargado del tratamiento.

XIV. REFERENCIAS

Se detallarán todos los documentos que hubieran sido utilizados en la ejecución de la EIPD por el equipo de trabajo.

No se trata de completar este apartado con una lista de documentos que hubieran podido ser utilizados sino de reflejar a lo largo de la EIPD documentos de referencia (dictámenes, sentencias, informes jurídicos, guías, referencias normativas, etc.) en los que la EIPD basa sus conclusiones, señalando en este apartado una relación exhaustiva de los documentos utilizados.

Por ejemplo, hacer referencia a un sistema de gestión de la seguridad de la información, a un determinado informe jurídico o dictamen que no hubieran sido utilizados en la EIPD, puede suponer, proporcionar información incorrecta al responsable quien basará sus decisiones en dicha información incorrecta, y en el caso de que dicha información se proporcione a una Autoridad de Control se podrá concluir que la información proporcionada es incompleta, incorrecta y, por tanto, inexacta, sin perjuicio del quebrantamiento de otros principios como el de transparencia.

XV. ANEXOS

Cualquier referencia a documentos de trabajo que pudieran haber sido incluidos en la EIPD que justifiquen las decisiones del responsable con relación al tratamiento y que, además, formen parte de los documentos con los que el responsable puede demostrar cumplimiento (evaluación del riesgo residual para los derechos y libertades, cláusulas contractuales, declaraciones, descripciones, informes, estándares, guías o documentos en general, inventario de activos, medidas de seguridad aplicables, etc.).

En …….. a …… de …….. de 202x

Firma en nombre de la entidad responsable del tratamiento

D./Dª.:

Cargo:

Correo electrónico:

Teléfono:

Firma del/de la Delegado/a de Protección de Datos (en su caso)

D./Dª.:

Correo electrónico:

Teléfono: