MODELO DE INFORME DE EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS (EIPD) PARA ADMINISTRACIONES PÚBLICAS

Este modelo de informe está orientado a cumplir con las previsiones del Reglamento General de Protección de Datos que incluye, entre las obligaciones del responsable del tratamiento, la necesidad de evaluar el impacto de las actividades de tratamiento en la protección de datos personales cuando resulte probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas.

Si bien este modelo no está orientado a los tratamientos de bajo riesgo, en aquellos casos en los que no es obligatoria la realización de una EIPD puede tenerse en cuenta la posibilidad de llevar a cabo este análisis con el objeto de estudiar en profundidad un tratamiento y sus procesos asociados necesarios para la consecución de los objetivos de una organización.

Este modelo contiene los capítulos y apartados que han de ser tenidos en cuenta para la elaboración del informe de una EIPD ya que, de alguna manera, son elementos que directa o indirectamente se relacionan con el análisis de un tratamiento.

Este modelo de informe está basado en las siguientes guías y normas:

- La Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD de la AEPD.

- Normas ISO-29134 “Directrices para la evaluación de impacto sobre la privacidad”, ISO-31000 “Gestión del riesgo. Principios y directrices” e ISO-31010 ““Gestión del riesgo. Técnicas de evaluación de riesgos”.

Versión de 9 de julio de 2019

I. RESUMEN EJECUTIVO

Este resumen debe tratar de forma condensada los aspectos más significativos de los capítulos que se desarrollan a lo largo del documento.

Contendrá la identificación del responsable-RGPD del tratamiento, de la unidad responsable en la organización, unidades gestoras de los datos que intervienen en alguna de las fases del tratamiento, encargados del tratamiento y subencargados del tratamiento.

A su vez, incluirá una breve descripción del tratamiento, su finalidad, las principales categorías de datos y su planeada implementación.

También destacará los factores de riesgo que motivan la realización de la EIPD y, en caso de no ser necesaria la EIPD, una exposición de los motivos por los que el responsable decide llevar a cabo la EIPD.

Finalmente, incluirá una breve descripción sobre el contexto de la EIPD como la metodología utilizada, la extensión y límites de la EIPD, los principales riesgos de privacidad identificados, los beneficios del tratamiento, las soluciones de gestión y técnicas planeadas, el análisis coste-beneficio 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. DESCRIPCIÓN DEL TRATAMIENTO

FECHA DE REALIZACIÓN DE LA EIPD

Fecha, hora, versión e identificación de quien coordina el equipo que lleva a cabo la EIPD.

Versión o revisión de la EIPD, versión del tratamiento (RAT o inventario).

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

NOMBRE Y DESCRIPCIÓN DEL TRATAMIENTO

Nombre interno dado al tratamiento, denominación del mismo en el inventario de tratamientos al que refiere el artículo 31.2 de la LOPDGDD, 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).

CATEGORÍAS DE DATOS

Incluirá una breve descripción introductoria de las categorías de datos tratados, incluyendo las operaciones realizadas sobre estos en cada una de las etapas o fases en las que se divide el tratamiento.

IDENTIFICACIÓN DEL RESPONSABLE-RGPD

Identificación de la Entidad Responsable-RGPD y si procede identificación de corresponsables.

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 las AA.PP. será de forma obligatoria el DPD.

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

IDENTIFICACIÓN DE TERCEROS IMPLICADOS EN EL TRATAMIENTO

Este apartado se completará en función de cómo esté planificada la implementación del tratamiento, así como la forma y extensión de las relaciones contractuales o cualquier otro instrumento jurídico vinculante (convenios, protocolos, instrucciones, etc.).

Identificación de las entidades que ejercen el rol de Encargado/Subencargado-RGPD

Identificación de POC en la Entidad Encargado/Subencargado (si cabe DPD)

CONTEXTO INTERNO DEL TRATAMIENTO EN LA ORGANIZACIÓN

Estructura de la organización, funciones y competencias. Políticas, normas y estándares adoptados, objetivos de madurez de la organización y en general la cultura de la organización. Señalar algunas de las características de la organización, como, por ejemplo, el número de personas implicadas en el tratamiento, sus perfiles, roles y la posible segregación de funciones a lo largo de todo el ciclo de vida del tratamiento. Incluir las características de los locales que puedan tener incidencia en los procesos de recogida de datos o de su tratamiento, como salas comunes para atención a los ciudadanos, lugares de trabajo en los que se comparte espacio de pantallas, teléfonos, etc. Identificación de todos los procesos de la organización que pueden estar relacionados o afectados por el tratamiento en relación al mapa de procesos de la misma. Contexto del sistema/s propuesto/s para la implementación del tratamiento y detalle de las tecnologías empleadas.

CONTEXTO EXTERNO DE LA ORGANIZACIÓN Y EL TRATAMIENTO.

En este apartado se describirá el entorno en el que la entidad despliega el tratamiento, pudiendo entenderse, entre otros, entorno social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, a nivel internacional, nacional, regional o local. En particular, la interacción del tratamiento con otros tratamientos externos a la organización, con los sujetos de los datos y los interesados.

IV. LICITUD DEL TRATAMIENTO Y CUMPLIMIENTO NORMATIVO

En este capítulo se desarrolla la base jurídica y, en su caso, normas y/o supuestos habilitantes. Hay que ser conscientes que el cumplimiento normativo no entra a formar parte del análisis de riesgos, sino que el cumplimiento de principios y derechos 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. Para completar este apartado se recomienda consultar la “Lista de Cumplimiento Normativo” publicada por la AEPD en: https://www.aepd.es/media/guias/guia-listado-de-cumplimiento-del-rgpd.pdf

V. METODOLOGÍA DE LA EIPD

IMPLICADOS EN LA EJECUCIÓN DE LA EIPD

Definición del equipo de trabajo, roles, tareas, responsabilidades, etc.

En general, el equipo de trabajo será multidisciplinar y dará respuesta al contexto en el que la EIPD y el tratamiento tienen lugar, contexto en el que podrán incluirse cuestiones normativas, sociales, culturales, etc.

En el caso de que el tratamiento implique el uso de tecnologías emergentes e innovadoras, se contará con perfiles de carácter tecnológico capaces de describir el alcance, tanto desde el punto de vista funcional como desde el posible impacto a la privacidad, de la tecnología utilizada.

GUÍAS, HERRAMIENTAS, METODOLOGÍAS, NORMAS Y DICTÁMENES UTILIZADOS EN LA EVALUACIÓN

Detalles sobre las metodologías utilizadas y justificación por la que se utilizan, incluyendo normas de obligado cumplimiento, si existen, con relación a la forma en la que se lleva a cabo la EIPD en este tratamiento en concreto.

También se incluirán aquellos dictámenes, sentencias, resoluciones o informes jurídicos que pudieran tenerse en cuenta como posibles criterios aplicables al tratamiento o a alguno de los aspectos del tratamiento en cualquiera de sus fases.

EXTENSIÓN Y LÍMITES DE LA EIPD: IDENTIFICAR QUE HA QUEDADO FUERA DE LA EVALUACIÓN

Se deberá de indicar los motivos por los que se limita el alcance de la EIPD incluyendo aquellos aspectos que quedarían fuera 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.

VI. ANÁLISIS DEL TRATAMIENTO

Este análisis supone estudiar el tratamiento dividiéndolo en etapas o fases desde el punto de vista del ciclo de vida de los datos.

En el Anexo I de la Guía de EIPD de la AEPD hay un modelo en el que se lleva a cabo una posible segmentación de los tratamientos en lo que se denomina “ciclo de vida de los datos asociados a un tratamiento”.

Es recomendable tener en cuenta, al menos, las fases de: captura, clasificación y almacenamiento, uso y tratamiento o explotación de los datos, cesiones y transferencias a terceros para su tratamiento, y destrucción de los datos.

Para cada una de las fases hay que identificar los elementos de riesgo inherentes en cada una de las etapas del tratamiento, en particular:

- Los propósitos y los efectos directos o deseados

- Los posibles efectos colaterales que puedan afectar a los derechos y libertades de los ciudadanos.

- Identificar categorías de datos, de interesados, modos de recogida y enriquecimiento de datos.

- Extensión en el tiempo, en el espacio, sobre un colectivo específico o en la información sobre un sujeto.

- Tecnologías y técnicas empleadas y su incertidumbre.

- Limitaciones a derechos, acceso a servicios u otros efectos de carácter jurídico.

- Intervinientes y bases jurídicas que legitiman su intervención en el tratamiento (contrato, obligación legal, etc.)

- Etc.

Los datos se organizan por su tipología atendiendo a características comunes a los mismos. Un análisis detallado analizaría cada campo de los datos de forma individual, siendo más práctico, se pueden agrupar tipos de datos.

VII. ANÁLISIS DE LA OBLIGACIÓN DE REALIZAR UNA EIPD: EVALUACIÓN DEL RIESGO

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 apartado Motivación para Realizar una EIPD).

Dicha lista, propuesta por la AEPD, está en proceso de aprobación en el Comité Europeo de Protección de Datos.

ANÁLISIS DE LA INCLUSIÓN DEL TRATAMIENTO EN LOS CASOS DE TRATAMIENTOS OBLIGADOS

En este apartado se determinará si hay una 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 35.2 del RGPD.

- Cumple con las condiciones que se detallan en la lista de tratamientos obligados (artículo 35.4 del RGPD) que puede consultarse aquí.

- Se dan los supuestos de mayor riesgo de los casos enumerados en el artículo 28.2 de la LOPDGDD.

EVALUACIÓN DEL NIVEL DE RIESGO

En este apartado se evalúa el nivel de riesgo, aunque el tratamiento no esté incluido en la casuística de tratamientos obligados.

Es necesario realizar un análisis del riesgo intrínseco, de acuerdo con el artículo 35.7.c del RGPD, teniendo en cuenta los elementos identificados durante el capítulo “Análisis del Tratamiento” para determinar e identificar los elementos de riesgo para los derechos y libertades de las personas, tanto los inherentes al tratamiento como los que se derivan del entorno en los que se desenvolverá el tratamiento.

Como resultado debemos tener una medida del nivel de riesgo para el tratamiento.

MOTIVACIÓN PARA REALIZAR LA EIPD

Motivos que dan lugar a la EIPD con independencia de que no exista una obligación de llevar a cabo la misma. Algunas razones que podrían ser tenidas en cuenta son:

- Generar conocimiento y cultura de protección de datos en la organización

- Análisis o auditoría de los tratamientos de una organización

- Mejora de la gestión global de los procesos de una organización

- Control sistemático, metódico y documentado del nivel de riesgo asumido en cada tratamiento.

- Ejercicio de la responsabilidad proactiva (accountability)

VIII. ANÁLISIS DE LA NECESIDAD DEL TRATAMIENTO

El propósito de este capítulo es realizar:

- El Juicio de Idoneidad: si la medida puede conseguir el objetivo propuesto;

- El Juicio de Necesidad: determinar si el tratamiento es necesario, en el sentido de que no existe otra menos invasiva para la privacidad para conseguir este propósito con la misma eficacia o con una eficacia razonable.

BENEFICIOS PARA LOS INTERESADOS

En este apartado se deberán identificar los beneficios directos para el conjunto de la sociedad y para los sujetos concretos sobre los que se tratan los datos. Por lo tanto, será necesario distinguir, si se da el caso, para el tratamiento concreto:

- Beneficios directos y objetivos para los sujetos sobre los que inciden los riesgos.
- Beneficios globales para la sociedad
- Mejor servicio para todos los ciudadanos y/o los sujetos bajo riesgo
- Mayor accesibilidad a la información
- Mayor sostenibilidad medioambiental
- Mayor transparencia en el tratamiento de los datos
- Mejora sustancial de la salud para los ciudadanos y/o los sujetos bajo riesgo
- Ayuda y protección a personas en situación de riesgo o desfavorecidas
- La protección frente a amenazas para la seguridad del Estado, la defensa o la seguridad pública.
- Aumentar la eficacia de los servicios a los ciudadanos y/o los sujetos bajo riesgo
- Servicios públicos más accesibles e integradores.
- Disminuir la discriminación (por género, por edad, por nacionalidad, por discapacidad, etc)

- Empoderamiento del ciudadano.

BENEFICIOS PARA LA ENTIDAD O LAS AA.PP. EN GENERAL

Este apartado se enumeran los beneficios que la implementación del tratamiento tiene para la entidad en sí.

- Cumplimiento normativo
- Mejora de la eficiencia
- Reducción de costes
- Incremento del control de las actuaciones de las AA.PP.
- Mejora del factor de transparencia para el responsable
- Mejora de la seguridad de las entidades
- Mejora de imagen
- Etc.

ALTERNATIVAS AL TRATAMIENTO Y POR QUÉ NO SE HAN ELEGIDO.

En los casos de tratamientos de alto riesgo, en este apartado hay que evaluar por qué no se han elegido otras alternativas a la forma de diseñar e implementar el tratamiento que implican un menor riesgo.

Para el caso de que sea una mejora, extensión o modificación de un tratamiento, es necesario señalar las ventajas de la nueva aproximación al tratamiento y que la finalidad que se persigue no se puede conseguir por otros medios, por ejemplo:

- Utilizando otros datos

- Reduciendo el universo de personas afectadas (de manera cuantitativa o cualitativa)

- Minimizando los datos recogidos, su uso o conservación.

- Haciendo uso de otras tecnologías menos invasivas

- o bien aplicando otros procedimientos o medios de tratamiento (modificando los inicialmente previstos), etc.

Para cada alternativa o forma de tratar anterior:

- Variación en las ventajas para la AA.PP.
- Variación en las ventajas para los ciudadanos
- Variación en los riesgos para los ciudadanos
- Ponderación de la alternativa frente al tratamiento propuesto y conclusión por la que se ha descartado.

IX. MEDIDAS PARA LA REDUCCIÓN DEL RIESGO

OPTIMIZACIÓN DEL TRATAMIENTO

Sobre los parámetros de descripción del tratamiento se ha de optimizar, desde el punto de vista de protección de datos, la descomposición de este en etapas o subprocesos, para poder realizar una aplicación con más granularidad sobre 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.

MEDIDAS PBDD

Las medidas de Privacidad por Defecto y desde el Diseño 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.

Una lista, no exhaustiva, se deriva de las expresadas en el artículo 25 del RGPD directamente relacionadas con las estrategias de privacidad implantadas tanto en el propio tratamiento de los datos como en la definición e implementación de los procesos involucrados en dichos tratamientos:

- MINIMIZACIÓN
- Eliminación temprana de los datos no necesarios.
- Minimización de los datos recogidos y tratados en cada etapa del tratamiento.
- Minimización de la frecuencia de recogida de los datos, por ejemplo, en lecturas de consumo, de geolocalización, etc.
- Reducción de la precisión/granularidad de recogida de los datos, por ejemplo, información de ocurrencia de eventos, posición, etc.
- Limitación de la accesibilidad de bases de datos a través de la red
- Anonimización temprana
- Seudoanonimización de los datos almacenados.
- Seudoanonimación de los datos en alguno de los subprocesos del tratamiento
- OCULTACIÓN
- Anonimización temprana
- Seudoanonimización de los datos almacenados.
- Seudoanonimación de los datos en alguno de los subprocesos del tratamiento
- Introducción de medidas perturbativas en los datos de origen
- Control de la privacidad de los metadatos en las comunicaciones electrónicas
- Uso de credenciales basadas en atributos

- Cifrado de la información almacenada o en tránsito
- SEPARACIÓN
- Compartimentación del acceso a los datos en el tiempo
- Compartimentación del acceso a los datos entre tratamientos.
- Particionamiento por atributos de las bases de datos
- Bloqueo de los datos
- Separación física de las fuentes de datos.
- AGREGACIÓN
- Generalización de datos personales
- Agregación de registros
- Reducción de la precisión/granularidad de recogida de los datos, por ejemplo, información de ocurrencia de eventos, posición, etc.
- Aplicación de diferenciales de privacidad en la difusión/acceso a los resultados del tratamiento
- INFORMACIÓN
- Transparencia de la extensión del tratamiento para el sujeto de los datos.
- Transparencia sobre el momento en el que se está realizando una recogida de datos
- CONTROL
- Control del usuario de la recogida de sus datos personales
- Control del usuario del tratamiento de sus datos
- Cifrado de la información extremo-extremo
- CUMPLIMIENTO
- Fijar requisitos de privacidad en los productos/servicios adquiridos o encargados para su desarrollo.
- Incorporar en el proceso de desarrollo de tratamientos que involucran datos personales los requisitos de privacidad en las primeras fases del ciclo de vida.
- Implementar procedimientos para garantizar la autenticidad o calidad de datos
- Implementación de medidas físicas para limitar la recogida de datos, como máscaras físicas de privacidad en cámaras, pestañas en webcams, etc.
- Configuraciones de privacidad máximas por defecto
- Especial atención a las circunstancias de sujetos en situación de especial riesgo o vulnerabilidad
- Limitación de tratamientos automáticos de datos que impliquen decisiones automatizadas

- DEMOSTRACIÓN DEL CUMPLIMIENTO
- Documentación de todas las decisiones tomadas en relación al tratamiento.
- Auditar el cumplimiento del RGPD en productos/servicios/componentes adquiridos o procesos llevados a cabo por terceros
- Adherirse a códigos de conducta o mecanismos de certificación.
- Medidas para garantizar la equidad en decisiones automatizadas
- Etc.

MEDIDAS DE *ACCOUNTABILITY*

Medidas de *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.

MEDIDAS DE SEGURIDAD

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 de los datos; 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.

Puede ser conveniente anexar al documento la Declaración de Aplicabilidad firmada por el responsable de seguridad.

X. ANÁLISIS DEL BALANCE ENTRE RIESGO-BENEFICIO

El objeto de este capítulo es realizar el Juicio de Proporcionalidad en sentido

estricto: determinar si el tratamiento es ponderado o equilibrado, porque se derivan más beneficios o ventajas para el interés general que no perjuicios sobre otros bienes o valores en conflicto.

La esencia de la gestión del riesgo es conseguir un correcto balance entre el coste y beneficio.

En el marco de una EIPD, el coste se traduce en los riesgos a los derechos y libertades que se somete a los sujetos cuyos datos son objeto de tratamiento.

Por lo tanto, es necesario encontrar el equilibrio entre los riesgos que el tratamiento bajo estudio implica para los sujetos de los datos, con los beneficios que este tratamiento aparta a la sociedad en su conjunto.

En función del resultado de la evaluación del riesgo y de las medidas aplicadas para su reducción y, por otro lado, teniendo en cuenta los beneficios que se derivan del tratamiento, justificar que las ventajas del tratamiento para los ciudadanos se compensan con los riesgos que corren los ciudadanos.

(Se supone que es un proceso cíclico en el que se van aplicando garantías que reducen dichos riesgos).

XI. PLAN DE ACCIÓN

En este capítulo se ha de reflejar el plan de implantación de las medidas y garantías para gestionar el riesgo y las acciones de seguimiento de la efectividad de las mismas

Una plantilla para realizar un plan de acción básico se encuentra en el Anexo IV de la Guía EIPD de la AEPD.

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 que se han definido para que la protección de datos sea una integral al producto/servicio, no una capa añadida.

XII. CONCLUSIONES Y RECOMENDACIONES

En este capítulo se establece el resultado final del análisis de riesgos, las directrices generales para la implementación del tratamiento, se determina si el riesgo es lo suficientemente bajo y si procede la Consulta Previa a la AEPD de acuerdo con el artículo 36 del RGPD.

XIII. ANEXOS

Aquellos contratos, declaraciones, descripciones, informes, referencias normativas, estándares, guías o documentos en general que sean relevantes para en la elaboración de los resultados de este informe y que se referencien en el texto

podrán incluirse como anexos de forma total o parcial.