SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

PRO.PD-05

PROCEDIMIENTO

DE ANÁLISIS DE RIESGOS Y EVALUACIÓN DE IMPACTO POTENCIAL

Diputación de Córdoba	DIPUTACIÓN DE CÓRDOBA

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	PRO.PD-05	DOCUMENTO:	PROCEDIMIENTO DE ANÁLISIS DE RIESGOS Y EVALUACIÓN DE IMPACTO POTENCIAL

REVISIÓN NÚMERO:	00	FECHA DE ENTRADA EN VIGOR:	15/11/2019

ES ORIGINAL:	☒	ES COPIA CONTROLADA:	☐	ES COPIA NO CONTROLADA:	☐

ELABORADOR POR:	REVISADO POR:	APROBADO POR:
TIC4YOU SL	DAVID YUBERO REY DPD DIPUTACIÓN DE CÓRDOBA	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN
		FECHA:
		15/11/2019

CONTROL DE CAMBIOS:

REVISIÓN Nº:	FECHA:	APARTADO MODIFICADO:	CAUSA DEL CAMBIO:	ENTRADA EN VIGOR:

DOCUMENTACIÓN OBSOLETA:	☐	FECHA:	

CLASIFICACIÓN DE LA INFORMACIÓN:

PÚBLICA:	☐	PUBLICABLE:	☒	USO INTERNO:	☐	CONFIDENCIAL:	☐	SECRETA:	☐

Í N D I C E

1. OBJETO

El objeto de este procedimiento es definir la sistemática a utilizar para la realización del análisis de riesgos en la Diputación de Córdoba junto con el Instituto Provincial de Bienestar Social, el Instituto Provincial de Cooperación con la Hacienda Local, el Instituto Provincial de Desarrollo Económico, el Consorcio Provincial de Prevención y Extinción de Incendios, el Patronato Provincial de Turismo de Córdoba, la Agencia Provincial de la Energía, la Fundación Provincial de Artes Plásticas Rafael Botí, la Empresa Provincial de Aguas de Córdoba, la Empresa Provincial de Residuos y Medio Ambiente y la Empresa Provincial de Informática (en adelante, la Diputación de Córdoba y su sector público institucional) y en función de los resultados de la misma definir la evaluación del impacto sobre la protección de datos.

2. ALCANCE

Este procedimiento es de aplicación a todos los responsables o encargados de tratamiento que, de conformidad con el artículo 35 del REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del consejo de 27 de abril de 2016 relativo a la Protección de las Personas Físicas en lo que respecta al tratamiento de Datos Personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos-RGPD), al realizar operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas, tengan la obligatoriedad de realizar una evaluación de impacto relativa a la protección de datos con el fin de valorar la particular gravedad y probabilidad del alto riesgo. La realización de dicho análisis de riesgos y evaluación de impacto se fundamentan de la misma manera en base a los considerandos, 74,75 76, 84, 89, 90 y 91 del propio RGPD y al artículo 28 apartado 1 de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.

3. REFERENCIAS

Para la elaboración de este procedimiento se ha utilizado como referencia:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Artículo 7 Condiciones para el consentimiento apartado 3, artículos 8, 9 y considerandos 32, 33, 38, 40, 42 y 43*.
- Corrección de errores del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- ISO/IEC 27005:2011 Tecnologías de la Información – Técnicas de Seguridad – Gestión de riesgos de seguridad de la Información.
- ISO 31010 de Gestión y Evaluación de Riesgos.
- ISO 29134 Tecnologías de la información - Guías para las Evaluaciones de Impacto en la Protección de los Datos.
- WP248 Guía sobre las Evaluaciones de Impacto en Protección de datos – Grupo Europeo Artículo 29
- Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD publicada por la AEPD.
- Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD publicada por la AEPD.

4. RESPONSABILIDADES

La responsabilidad del procedimiento recae de manera directa en la Diputación de Córdoba y en su sector público institucional como responsable del tratamiento, que será quien lleve a cabo el análisis de riesgos y evalúe la idoneidad de realizar la evaluación de impacto en función de la clasificación de riesgo resultado del análisis. El DPD deberá estar en conocimiento de los resultados del análisis de riesgos realizado y deberá proporcionar el asesoramiento necesario al responsable del tratamiento para la evaluación de impacto relativa a la protección de datos.

5. DESARROLLO

5.1. ANÁLISIS DE RIESGOS

El análisis de riesgos para un determinado tratamiento permite identificar los riesgos que se ciernen sobre los datos de los interesados y establecer una respuesta adoptando las salvaguardas necesarias para reducirlos hasta un nivel de riesgo aceptable.

5.1.1. CONSIDERACIONES GENERALES

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

Una amenaza es cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesado sobre cuyos datos de carácter personal se realiza un tratamiento. Según la Agencia Española de Protección de Datos, las amenazas se pueden categorizar principalmente en tres tipos:

- Acceso ilegítimo a los datos. Que afecta a la CONFIDENCIALIDAD.
- Modificación no autorizada de los datos. Que afecta a la INTEGRIDAD.
- Eliminación de los datos. Que afecta a la DISPONIBILIDAD.

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

La evaluación de los riesgos debe ser el resultado de una reflexión sobre las implicaciones que los tratamientos de datos de carácter personal tienen sobre los interesados. Se trata de establecer hasta qué punto una actividad de tratamiento, por sus características, el tipo de datos a los que se refiere o el tipo de operaciones puede causar un daño a los interesados.

5.1.2. EJECUCIÓN

La Diputación de Córdoba y su sector público institucional llevarán a cabo el análisis de riesgo de cada uno de los tratamientos de información que estén recogidos en el registro de actividades de tratamiento RG.PD-014. El responsable debe evaluar si las actividades de tratamiento entrañan un alto riesgo para los derechos y libertades del interesado. con el objetivo de determinar si se requiere una evaluación de impacto relativa a la protección de datos (EIPD).

En caso de que se detecten tratamientos que entrañan un riesgo elevado para los derechos y libertades del interesado, el responsable llevará a cabo una evaluación de impacto. Si por el contrario, el responsable determina que no es necesaria la evaluación de impacto debe documentar y justificar la no realización de dicha evaluación.

5.2. EVALUACIÓN DE IMPACTO

5.2.1. CONSIDERACIONES GENERALES

La Evaluación de Impacto en la Protección de Datos Personales es una herramienta con carácter preventivo que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos. De esta forma, permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable. La Evaluación de Impacto es un proceso cíclico que debe entenderse de mejora continua, de este modo, el responsable debe revisar si los tratamientos siguen siendo conformes con la Evaluación a la que hubieran sido sometidos y, en todo caso, volver a repetirla cuando exista un cambio del riesgo del tratamiento.

5.2.2. EJECUCIÓN

La Evaluación de Impacto ha de realizarla el responsable del tratamiento con el asesoramiento por parte del DPD de Diputación de Córdoba y su sector público institucional. Una Evaluación de Impacto no se requiere siempre, en cada actividad de tratamiento, el responsable debe valorar la necesidad de llevar a cabo la misma.

El responsable de tratamiento decidirá si ha de realizarse una evaluación de impacto o no en función del análisis de cada actividad de tratamiento. Si el responsable determina que no es necesario llevarla a cabo, se entiende que las actividades de tratamiento no están expuestas a riesgos relevantes que motiven la necesidad de realizarla, no obstante, se debe documentar adecuadamente los motivos por

los cuales se ha llegado a esa conclusión. En cualquier caso, se debe mantener evidencia de que se ha llevado a cabo este análisis mediante la elaboración del análisis de riesgos.

Si por el contrario, el responsable determina la idoneidad de realizar una evaluación de impacto, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas deberá documentarlo.

El responsable está obligado a realizar una evaluación de impacto siempre que las actividades de tratamiento supongan:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.
- Tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 del RGPD.
- Observación sistemática a gran escala de una zona de acceso público.

La evaluación de impacto deberá incluir como mínimo:

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

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

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

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

Ante cambios en la descripción del tratamiento o en la experiencia que muestre amenazas o riesgos desconocidos hasta entonces (los fines y medios), se debe realizar una nueva evaluación de impacto, generar un nuevo informe y un plan de acción con las nuevas medidas de control. En caso de que los cambios sobre el tratamiento no sean significativos, y no generen por tanto nuevas amenazas y riesgos sobre los derechos y libertades de los interesados, igualmente se debe realizar una valoración de los cambios producidos y documentar claramente la no necesidad de implantar nuevas medidas de control adicionales.