PROTOCOLO DE ACTUACIÓN EN LA LÍNEA 4 DEL PLAN DE CONTROL E INSPECCIÓN SOBRE PROTECCIÓN DE DATOS EN EL SECTOR PÚBLICO ANDALUZ 2023-2025 DEL CONSEJO DE TRANSPARENCIA Y PROTECCIÓN DE DATOS DE ANDALUCÍA

Por Resolución de 20 de septiembre de 2023 se aprobó el Plan de Control e Inspección sobre Protección de Datos en el Sector Público andaluz 2023-2025 del Consejo de Transparencia y Protección de Datos de Andalucía.

El apartado segundo de la Resolución mencionada establece que para el adecuado desarrollo de cada una de las líneas de actuación del Plan, se elaborará un protocolo en el que se describan los objetivos generales y detallados de las mismas, los criterios para la selección de las entidades directamente afectadas, la metodología a emplear para su desarrollo y el calendario previsto para su realización.

Por su parte, el Plan incluye como Línea 4 de actuación la "Comprobación de realización de análisis de riesgos y evaluaciones de impacto por parte de los responsables de tratamiento".

Mediante este documento, se procede a dar cumplimiento a lo indicado en el apartado segundo.

Primero. Objetivos generales y detallados.

El objetivo general de esta Línea del Plan consiste en comprobar el cumplimiento por parte de los responsables del tratamiento de la obligación de realizar análisis de riesgos de los tratamientos de datos personales, y en su caso de evaluaciones de impacto, así como verificar la metodología empleada y el plan de tratamiento de riesgos adoptado en el marco de la responsabilidad proactiva.
En concreto, el análisis debe considerar factores como la correcta identificación de los tratamientos que se llevan a cabo, la naturaleza de los datos personales, la forma en que se recopilan y procesan y las posibles amenazas o vulnerabilidades en términos de origen, naturaleza, probabilidad y gravedad. Una vez evaluados los riesgos inherentes al tratamiento, el responsable aplicará medidas para mitigarlos a fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el RGPD.

Los objetivos específicos son los siguientes:

- Seleccionar de entre los sujetos obligados aquellas entidades cuyos Inventarios de actividades de tratamiento formarán la muestra.
- La correcta identificación de los tratamientos que se llevan a cabo por el responsable.
- Verificar la realización, metodología y documentación del análisis de riesgos.
- Identificar aquellos tratamientos que deberían disponer de una evaluación de impacto relativa a la protección de datos y comprobar su realización, metodología y documentación asociada.
- Verificar la realización, documentación y estado de cumplimiento del plan de tratamiento de riesgos adoptado.

Segundo. Criterios para la selección de los inventarios de actividades de tratamiento

De conformidad con lo establecido en el Plan de Control e Inspección, el ámbito de esta actuación afectará a una muestra aleatoria de al menos 20 inventarios de tratamientos de responsables de la Administración de la Junta de Andalucía y organismos autónomos, entidades públicas empresariales, agencias y demás entes públicos vinculados o dependientes de la Administración autonómica; Universidades; Diputaciones provinciales andaluzas; municipios que sean capitales de las provincias andaluzas y municipios que, sin ser capitales de provincia, preferentemente tengan una población superior a 100.000 habitantes.

Por otra parte, el punto 2 del apartado segundo de la Resolución por la que se aprueba el Plan establece que:
"*El Área de Protección de Datos podrá ampliar la muestra de entidades a inspeccionar en cada una de las Líneas, de acuerdo con los criterios de selección fijados en los correspondientes protocolos*."

Una vez realizado un trabajo previo de análisis de la publicación que realiza la Administración de la Junta de Andalucía de sus actividades de tratamiento[1], se considera que es conveniente concretar el ámbito de actuación del Plan en la citada organización, a través de unos adecuados criterios de elección de la muestra, de cara al mejor cumplimiento de los objetivos del mismo.

En el caso de las Consejerías de la Junta de Andalucía, debe tenerse en cuenta que lo habitual es el establecimiento de políticas de protección de datos y metodologías de trabajo comunes a toda la Consejería, en particular en lo relativo al Registro de actividades de tratamiento y al análisis de riesgos que en su caso se llevase a cabo, así como la implementación homogénea de las medidas técnicas y organizativas siguiendo criterios normalizados para mitigar los riesgos. En el mismo sentido, la designación del delegado de protección de datos suele realizarse a nivel de toda la Consejería, sirviendo como punto de referencia para todos los órganos de la misma.

Por ello y en aras de una mejor consecución del objetivo fijado en esta línea de comprobar el cumplimiento de la realización del análisis de riesgos de los tratamientos de datos personales en la Administración de la Junta de Andalucía, a los efectos de determinar una muestra suficientemente representativa, se estima oportuno incluir como criterio de selección los inventarios de tres responsables de tratamiento para cada una de las Consejerías seleccionadas según el criterio expuesto a continuación. Tal criterio hace que el número de inventarios de tratamientos de responsables sea superior a los veinte establecidos como mínimo para esta línea de actuación.

Para la selección de la muestra se seleccionarán de forma aleatoria:

- Los inventarios de 3 responsables del tratamiento pertenecientes a 3 Consejerías de la Junta de Andalucía. Tanto la Consejerías, como los responsables pertenecientes a las mismas se seleccionarán aleatoriamente.
- 3 inventarios de responsables del tratamiento pertenecientes a organismos autónomos, entidades públicas empresariales, agencias y demás entes públicos vinculados o dependientes de la Administración autonómica.

1 Se publica en https://juntadeandalucia.es/protecciondedatos/buscador

- 3 inventarios de responsables del tratamiento pertenecientes a universidades públicas andaluzas
- 3 inventarios de responsables del tratamiento pertenecientes a Diputaciones provinciales andaluzas.
- 5 inventarios de responsables del tratamiento pertenecientes a ayuntamientos capitales de provincia.
- 3 inventarios de responsables del tratamiento pertenecientes a ayuntamientos con una población superior a 100.000 habitantes que no sean capitales de provincia.

La persona responsable del Gabinete de Cumplimiento levantará diligencia en la que se incluyan los responsables del tratamiento y, en su caso, las Consejerías seleccionadas.

Tercero. Metodología a utilizar en el desarrollo de las actuaciones.

Tras la selección de los responsables del tratamiento, se procederá a remitirles comunicación informando de la aprobación del Plan y del inicio de la actuación inspectora requiriéndole la siguiente información relativa al Inventario de actividades de tratamiento (se indicará la url que se toma como referencia de dicho Inventario, o en caso de no encontrarse, se requerirá su ubicación):

- Confirmación de la existencia de análisis de riesgos para los tratamientos contemplados en el Inventario.
- Documentación relativa a dichos análisis de riesgos.
- Descripción del procedimiento y metodología empleada para realizar dichos análisis de riesgos así como para identificar los tratamientos expuestos a dichos riesgos.
- Identificación de los tratamientos que disponen de una evaluación de impacto y la documentación generada.
- Confirmación de la existencia y documentación asociada al plan de tratamiento de los riesgos (entendido como el conjunto de medidas adoptadas o planificadas para mitigar los riesgos) así como información relativa al estado de ejecución de dicho plan de tratamientos.

Se concederá un plazo de un mes para que el requerimiento sea atendido, con advertencia expresa de que, "*en virtud de los poderes de investigación otorgados a las autoridades de control por el artículo 58.1 del RGPD, así como de lo dispuesto en el artículo 16.5 del Decreto 434/2015, de 29 de septiembre, por el que se aprueban los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía, el responsable y el encargado del tratamiento de los datos de carácter personal tienen la obligación de facilitar los documentos, informaciones y cualquier otra colaboración que se precise para realizar la función de investigación por parte de este Consejo, como autoridad de control en la materia*".

El responsable del tratamiento podrá realizar las consultas al Consejo que estime necesarias a través del correo electrónico del área "*protecciondedatos.ctpda@juntadeandalucia.es*".

No obstante el carácter eminentemente sensibilizador y preventivo del Plan, si transcurrido el plazo concedido el responsable del tratamiento no hubiera proporcionado la información requerida, se reiterará dicho requerimiento, otorgando un plazo adicional de 15 días, advirtiendo de la incoación de un

procedimiento sancionador por una infracción muy grave de acuerdo con lo establecido en el artículo 72 letra o) de la LOPDGDD, por la resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos competente en caso no ser atendido.

Para cada responsable del tratamiento, de acuerdo con la información proporcionada, se evaluará el análisis de riesgos, las evaluaciones de impacto y el plan de tratamiento de riesgos de la siguiente forma.

En relación al análisis de riesgos, se evaluarán los siguientes conceptos:

- El inventario de actividades de tratamiento refleja correctamente los tratamientos realizados por el responsable del tratamiento
- La existencia del análisis de riesgos o de documentación asociada
- Los tratamientos del inventario cubiertos por el análisis de riesgos
- Las amenazas contempladas en el análisis de riesgos
- El análisis de riesgos se realiza de acuerdo con una metodología sistemática
- El análisis de riesgos permite identificar el nivel de riesgo de las operaciones de tratamiento y en particular si el riesgo es alto

En relación a las evaluaciones de impacto, se evaluarán los siguientes conceptos:

- La existencia de una evaluación de impacto para los tratamientos que entrañen alto riesgo (una única evaluación podrá abordar una serie de tratamientos similares que entrañen altos riesgos similares) o de documentación asociada
- Las evaluaciones de impacto contienen como mínimo el contenido exigido en el art.35.7 RGPD
- Las evaluaciones de impacto se realizan siguiendo una metodología establecida
- Las evaluaciones de impacto contienen un conjunto adecuado de medidas previstas para afrontar los riesgos y tras su determinación, el riesgo residual es aceptable (no es alto)

En relación al plan de tratamientos de riesgos, se evaluarán los siguientes conceptos:

- Existencia del plan de tratamiento de riesgos o de documentación asociada
- La adecuación de las medidas técnicas y organizativas adoptadas o planificadas al nivel de riesgo identificado
- Las medidas técnicas y organizativas adoptadas o planificadas se enmarcan en el Esquema Nacional de Seguridad
- El nivel de ejecución del plan y el control sobre su grado de avance

De cada evaluación realizada, se elaborará un informe que será trasladado al responsable del tratamiento. En dicho informe se identificarán las posibles mejoras, o en caso de deficiencias, las actuaciones correctivas necesarias en la realización de análisis de riesgos, en la identificación de los tratamientos expuestos a dichos riesgos y en las evaluaciones de impacto, en su caso.

Los resultados obtenidos tras las actuaciones inspectoras se incluirán en la propuesta de informe final que el Área de Protección de Datos elevará a la Dirección del Consejo.

Cuarto. Calendario previsto.

Está previsto dividir el ámbito de la actuación en los dos años completos del Plan. Así, durante 2024 se abordará una mitad de la selección realizada y en 2025 la restante con el siguiente calendario previsto.

1. Selección de los responsables del tratamiento: febrero de 2024

2. Actuaciones inspectoras: marzo-octubre de 2024 y marzo-octubre de 2025

3. Informe de resultados: diciembre de 2024 y diciembre de 2025

En Sevilla, a la fecha de firma electrónica,

LA DIRECTORA DEL ÁREA DE PROTECCIÓN DE DATOS

Blanca Álvarez Yaque

Control de ediciones

N.º de edición	Fecha de la edición	Naturaleza de la edición
v3	04/10/2023	Edición inicial
v4	16/11/2023	Eliminación de la muestra la selección adicional aleatoria correspondiente a 20 ayuntamientos de municipios con una población entre 25.000 y 100.000 habitantes y adaptación del número aleatorio por tipología de la muestra para para mayor coherencia con el Plan de Inspección.
v5	07/02/2023	Inclusión en la muestra seleccionada de los inventarios de tres responsables del tratamiento pertenecientes a las Consejerías de la Junta de Andalucía, según se explica en el propio documento. Inclusión de mayor detalle sobre cómo se evaluará la documentación remitida por el responsable del tratamiento Selección de todos los responsables en febrero de 2024 para simplificar la ejecución de la Línea.