

011/2025**I**

Tal y como acertadamente resulta de la Exposición de Motivos, y de la Memoria de Análisis de Impacto Normativo (MAIN), el Real Decreto 311/2022, de 3 de mayo (RD 311/2022), por el que se regula el Esquema Nacional de Seguridad (ENS), tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de las relaciones entre la Administración Pública y los ciudadanos a través de los medios electrónicos, estableciendo los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada y los servicios prestados.

El RD 311/2022 requiere con carácter obligatorio (art. 12) a las diferentes Administraciones Públicas, y en concreto a cada Ministerio, (art. 12.3), que cuenten con una Política de Seguridad que será aprobada por la persona titular del Departamento. Esta Política de Seguridad constituye las Directrices que rigen la forma en que la organización gestiona y protege la información que trata y los servicios que presta (art. 12.1). Dicha Política de Seguridad deberá de incluir, como mínimo (art. 12.1): a) Los objetivos o misión de la organización; b) El marco regulatorio en el que se desarrollarán las actividades; c) Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación; d) La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización; e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso; y f) Los riesgos que se derivan del tratamiento de los datos personales.

En este último aspecto, relativo a los sistemas de información que traten datos personales, el art. 3 del RD 311/2022 no sólo determina que estas han de ser coherentes con lo establecido en el RGPD y la LOPDGDD, sino que establece prevenciones adicionales, por cuanto en esos casos prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto en materia de protección de datos que el responsable o encargado del tratamiento, asesorado por el Delegado de Protección de Datos,

ha de realizar, en caso de que dichas medidas resultaren agravadas respecto de las previstas en el real decreto.

Por lo que hace a la AEPD, esta ha tenido ya oportunidad en reiteradas ocasiones de examinar los diferentes proyectos de órdenes relativas a las políticas de Seguridad de diferentes ministerios, como pueden ser, entre las más cercanas, los Informes 036/2024, relativo a la política de seguridad del Ministerio de Cultura, o el Informe 040/2024, relativo a la política de seguridad del Ministerio de Hacienda.

II

Entrando ya en el contenido concreto del Proyecto relativo a la protección de datos personales, el art. 4.2, dentro de los “Principios particulares y responsabilidades específicas”, en su letra a) recoge como una directriz fundamental de seguridad que en esta materia de protección de datos personales se adoptarán las medidas técnicas y organizativas destinadas a garantizar una adecuada protección de los datos, y que tal y como se establece en el RGPD y la LOPDGDD, dichas medidas deberán ser apropiadas en función del análisis de riesgos, así como de una evaluación de impacto relativa a la protección de datos cuando sea probable que un tratamiento, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, lo que es conforme con lo requerido por el art. 3 del RD 311/2022, que ya se ha expuesto.

El art. 6 detalla la estructura organizativa en materia de seguridad de la información en el departamento, aspecto que el RD 311/2022 requiere en su art. 12, al referir que la política de seguridad deberá incluir, entre otros aspectos, los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación, así como la estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.

El art. 11 del RD 311/2022 establece que en los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema, y el art. 13 determina la responsabilidad de dichas figuras.

En el Proyecto se distinguen y desarrollan las funciones de dichas figuras (arts. 9, responsable de seguridad; 10, responsable de los sistemas; 11 responsable de la información; 12, responsable de los servicios),

En el art. 8 se establece el Comité de Seguridad de la Información del Departamento, en cuya composición se incluye a los Delegados/as de Protección de Datos del Departamento (DPD), los cuales “[a]ctuarán, con voz, pero sin voto para garantizar su independencia en atención a la naturaleza de sus funciones de apoyo y asistencia”. Esta función de asesoramiento, en la cual no tienen los DPDs una naturaleza decisoria en su participación en dicho Comité se informa favorablemente por esta AEPD, ya que sigue las recomendaciones realizadas por esta Agencia al informar reiteradamente otras Políticas de Seguridad de Información de otros departamentos ministeriales.

En el art. 9.4 se establece que la persona designada como Responsable de la Seguridad no podrá ser designada como Responsable de la Información, ni de los Servicios. Adicionalmente, deberá ser distinta del Responsable de los Sistemas y no podrá existir dependencia jerárquica entre ambos. Si bien en el art. 13.3 del Proyecto se recoge, adecuadamente, que a fin de garantizar su independencia y evitar cualquier tipo de conflicto de intereses en el ejercicio de sus funciones, no podrá coincidir en la misma persona la designación del DPD y el Responsable de Seguridad, se sugiere que se recoja igualmente en este apartado 9.4 esta incompatibilidad funcional con el DPD.

Igualmente se sugiere que en el art. 8.2.b), apartado iii, se establezca que se recogerá en acta el parecer del DPD si no coincide con la decisión adoptada por el Comité de Seguridad de la Información del Departamento.

En el art. 11.1 debe de recogerse la mención no sólo de la LO 3/2018, sino, además, la del RGPD, en cuanto que es la norma principal en materia de protección de datos.

En el art. 13 se regula la figura del Delegado/a de Protección de Datos. Aparte de la sugerencia ya señalada al comentar el art. 9.4 del Proyecto respecto de la incompatibilidad funcional entre el DPD y el Responsable de Seguridad, no se entiende muy bien la referencia final del apartado 1 del art. 13: (el DPD) “es único para el ámbito del Ministerio de Juventud e Infancia, *excluyendo los organismos públicos adscritos, sin perjuicio de la existencia de DPD en los mismos*”.

El art. 15 regula “las personas designadas Responsable y Encargado de tratamiento de datos personales”. En primer lugar, esta regulación no es en sí misma materia propia de la Política de Seguridad conforme al ENS (RD 311/2022) (ver art. 11.1). El responsable y el encargado del tratamiento son términos propios específicos de la materia de protección de datos personales,

siendo además términos definidos en el RGPD (art. 4.7 y 4.8), que los define así:

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

No hay necesidad por tanto de un precepto en este Proyecto que defina de nuevo estos términos, además de manera confusa al hacer mención, en primer lugar, a la “persona designada” responsable o encargado, como si fuera una circunstancia que ha de determinarse conforme a la Política de Seguridad (al igual que ha de designarse un responsable de seguridad, o de información etc.), y en segundo lugar porque la determinación de quién sea responsable del tratamiento vendará dado por quién determina verdaderamente los fines y medios del tratamiento, o bien cuando sea “establecido” dicho responsable del tratamiento por el Derecho de la Unión o de los Estados miembros, cuando este Derecho determina los fines y medios del tratamiento.

En cuanto al Encargado del tratamiento, este no se “designa” en virtud de la política de Seguridad, sino que es, como se ha definido en el RGPD, la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales *por cuenta* del responsable del tratamiento. Para ello, además, el tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable, en los términos del art. 28 RGPD.

En conclusión, se sugiere suprimir este artículo 15 del Proyecto.

El art. 16 está dedicado a la protección de datos de carácter personal. Esta Agencia informa favorablemente a dicho precepto, si bien observa lo siguiente: dado que se ha sugerido suprimir el art. 15 del Proyecto para evitar confusión con los términos del RGPD respecto de responsable y encargado/a del tratamiento, se sugiere que en el párrafo segundo del apartado 2 del art. 16 y en el apartado 4 se suprima la expresión “persona designada”, dejándose exclusivamente “responsable del tratamiento”.

Por lo que respecta al art. 17 (Resolución de conflictos), hay que abundar en la necesidad de suprimir el art. 15, por cuanto desde la perspectiva de protección de datos, el responsable del tratamiento es, como hemos visto, quien determina los fines y medios del tratamiento, por lo que mal puede comprenderse que el “responsable del tratamiento” pueda recibir indicaciones de un tercero respecto de dichos fines y medios del tratamiento (porque entonces ese tercero sería verdaderamente el “responsable del tratamiento”). Una vez suprimido el contenido del art. 15, el art. 17 sí cobra sentido, por cuanto la resolución de conflictos a que ha de atender la Política de Seguridad es la derivada del RD 311/2022 (no otra).

De todos modos, el RD 311/2022 menciona la resolución de conflictos en los arts. 6.4.j) y 14. En ambos preceptos, la resolución de los conflictos que puedan derivarse del establecimiento de la estructura organizativa de seguridad, así como aquellos conflictos de competencia que pudieran aparecer entre los diferentes centros directivos en materia de seguridad de la información, se encomiendan a la Comisión Ministerial de Administración Digital (CMAD) del Ministerio, órgano este creado y regulado por la Orden JUI/844/2024, de 31 de julio, por la que se crea la Comisión Ministerial de Administración Digital del Ministerio de Juventud e Infancia y se regula su composición y funciones. El art. 17 del Proyecto encomienda la resolución de conflictos “*al superior jerárquico*”. Esta solución parecería ser contraria a los citados arts. 6.4.j) y 14 del RD 311/2022, por lo que el art. 17 del Proyecto debería de acomodarse a ellos, estableciendo que la resolución de conflictos en esta materia de seguridad de la información corresponde a la CMAD.

Por último, tampoco se comprende muy bien la Disposición Final cuarta, vigencia, del Proyecto, por cuanto esta establece que: *La presente orden, así como su marco normativo aprobado, seguirá vigente en tanto en cuanto no sea aprobada la política de seguridad del departamento ministerial que asuma las competencias del Ministerio de Juventud e Infancia y se desarrolle la estructura normativa que garantice la seguridad de los activos tecnológicos y de información utilizados por los órganos superiores y directivos del actual Ministerio de Juventud e Infancia para el ejercicio de sus competencias*. Este Proyecto de Orden que se informa precisamente aprueba la política de seguridad del Ministerio de Juventud e Infancia, por lo que su redacción parece incongruente con la misma existencia del Proyecto, que, una vez aprobado, será la Política de Seguridad del Ministerio de Juventud e Infancia.