0033/2026

I

El borrador de Resolución (Resolución) tiene por objeto la aprobación de la Política de Seguridad de la Información (PSI) en el ámbito de la Administración Digital del Instituto de la Juventud (INJUVE), tal y como establece su artículo 1. La Resolución establece el marco organizativo global en materia de seguridad de la información del organismo, así como las directrices generales que rigen la gestión y protección de la información tratada y de los servicios electrónicos prestados.

El artículo 12.3 del Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad (ENS), prevé que los organismos públicos y las entidades integrantes del sector público institucional estatal puedan disponer de una política propia de seguridad de la información, aprobada por el órgano competente. Dicha previsión habilita al INJUVE para aprobar su propia PSI.

El citado precepto establece asimismo que, en tales supuestos, la política de seguridad deberá mantener coherencia con la del Departamento ministerial al que la entidad se encuentre vinculada, adscrita o de la que dependa, o bien quedar integrada dentro del ámbito subjetivo de aplicación de aquella. En este sentido, la PSI proyectada prevé expresamente su alineamiento con la Política de Seguridad de la Información del Ministerio de Juventud e Infancia, departamento al que se encuentra adscrito el INJUVE. La Política de Seguridad de la Información del Ministerio fue aprobada mediante la Orden JUI/29/2026.

En consecuencia, la previsión de alineamiento de la PSI del INJUVE con la política ministerial permite considerar satisfecha la exigencia de coherencia organizativa y funcional prevista en el artículo 12.3 del ENS.

II

En lo que atañe a la protección de datos de carácter personal, el apartado tercero de la Resolución establece el marco normativo aplicable a las actuaciones del INJUVE en materia de seguridad de la información en el ámbito de la prestación de los servicios electrónicos a los ciudadanos, incluyendo un conjunto de normas que configuran el entorno jurídico en el que se desenvuelve la PSI. En lo que aquí interesa, se remite expresamente al Reglamento (UE) 2016/679, de 27 de abril de 2016 (RGPD), y a la Ley

Orgánica 3/2018, de 5 de diciembre (LOPDGDD), en materia de protección de datos personales.

Asimismo, el apartado decimocuarto regula específicamente la protección de datos de carácter personal dentro de la PSI, integrando adecuadamente los principios y obligaciones derivados del RGPD y de la LOPDGDD. En este apartado se dispone que:

"*Decimocuarto. Protección de datos de carácter personal.*

1. En el ámbito del INJUVE, la garantía de la protección de datos de carácter personal de las actividades de tratamiento es un objetivo compartido por todas las unidades del mismo que se rige por los principios recogidos en el artículo 5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

2. La seguridad de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, constituye uno de los principios que deben regir su tratamiento, aplicándose para ello las medidas técnicas u organizativas apropiadas que garanticen un nivel de seguridad adecuado en función del correspondiente análisis de riesgos, tal y como se establece en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre. Dicho análisis de riesgos se realizará, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

El cumplimiento de este principio corresponde al Responsable del tratamiento que, adicionalmente, debe ser capaz de demostrarlo y aplicarlo de forma temprana en la fase de diseño del tratamiento y garantizando que su aplicación sea efectiva por defecto.

3. La garantía del cumplimiento de lo previsto en el apartado anterior, se articulará a través del marco organizativo establecido en la presente Política de Seguridad y se llevará a cabo de conformidad con la normativa aplicable en materia de protección referida en el artículo 2 de esta resolución y en el Real Decreto 311/2022, de 3 de mayo, prevaleciendo las medidas derivadas de la aplicación de la normativa de protección de datos cuando, tras un análisis de riesgos, se estime que las mismas son superiores a las previstas en el ENS.

4. La observación del principio de seguridad del tratamiento de los datos personales cobrará especial relevancia cuando sea probable que un determinado tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, en cuyo caso el Responsable del tratamiento recabará

el asesoramiento del DPD al realizar la preceptiva evaluación de impacto relativa a la protección de datos.

5. Las auditorías de seguridad previstas en el Esquema Nacional de Seguridad incorporarán la revisión de las medidas técnicas y organizativas de seguridad de los datos personales a las que se refiere este artículo."

En el apartado decimocuarto.1 se prevé el pleno sometimiento de los tratamientos de datos a los principios de protección de datos. En particular, recoge expresamente que la garantía de la protección de datos personales constituye un objetivo compartido por todas las unidades del organismo y que dicha actuación deberá regirse por los principios previstos en el artículo 5 del RGPD.

Debe valorarse igualmente de forma favorable la regulación contenida en el apartado decimocuarto.2 de la Resolución, en la medida en que incorpora expresamente los principios de responsabilidad proactiva y de protección de datos desde el diseño y por defecto previstos en los artículos 24 y 25 del Reglamento (UE) 2016/679. Asimismo, el citado apartado incorpora adecuadamente el principio de seguridad del tratamiento previsto en el artículo 32 del citado Reglamento, al establecer que deberán implantarse medidas técnicas y organizativas apropiadas atendiendo al correspondiente análisis de riesgos. La vinculación de dichas medidas al estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y fines del tratamiento, así como a los riesgos para los derechos y libertades de las personas físicas, resulta plenamente conforme con el modelo de cumplimiento basado en el riesgo que inspira la normativa europea de protección de datos.

En cuanto a la coordinación entre la normativa de protección de datos y el ENS, resulta especialmente relevante la previsión contenida en el apartado decimocuarto.3, con relación a la adopción de medidas técnicas u organizativas apropiadas que garanticen un nivel de seguridad adecuado en función del correspondiente análisis de riesgos, *dicha previsión* —que responde a lo establecido en el art. 3.3 del Real Decreto 311/2022, de 3 de mayo—, *se ha venido señalando en los informes emitidos por esta Agencia*, por todos el Informe 170/2018, de 12 de noviembre de 2018, que recordó la diferenciación entre la figura del Delegado de Protección de Datos (DPD) y el Responsable de Seguridad, que, por su interés al caso, reproducimos en lo procedente:

> *"Con carácter previo a analizar la concreta cuestión planteada en la consulta, este Gabinete Jurídico estima conveniente hacer una referencia previa a la diferenciación, sustantiva y competencial, que existe entre el ámbito de la seguridad de información y el de la protección de datos de carácter personal.*
>
> *Por lo que se refiere a la seguridad de la información, la misma comprende el conjunto de técnicas y medidas orientadas a garantizar la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para cualquier organización, independientemente del formato que tengan.*

En el ámbito de las Administraciones Públicas españolas y en relación con los sistemas que manejan información en formato electrónico (comúnmente denominados "Tecnologías de la Información y las Comunicaciones -TIC-"), el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, actualmente sustituido por el artículo 156.2 de la Ley 40/2015, de régimen jurídico del sector público, creó el Esquema Nacional de Seguridad, que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la citada Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

Dicho precepto encuentra su desarrollo reglamentario en el 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, cuyo Preámbulo señala que "la finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios" añadiendo que "en este contexto se entiende por seguridad de las redes y de la información, la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles".

En este ámbito, son múltiples los órganos que ostentan competencias, pudiendo destacarse, conforme a lo recogido en el reciente Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, al Centro Criptológico Nacional (CCN) responsable del citado ENS, el Instituto Nacional de Ciberseguridad (INCIBE) y el Ministerio de Defensa.

Por el contrario, la protección de datos de carácter personal de las personas físicas se configura como un auténtico derecho fundamental que encuentra su fundamento en el artículo 18.4 de la Constitución Española, conforme al cual "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Así lo ha reconocido nuestro Tribunal Constitucional, destacando en la Sentencia 94/1998, de 4 de mayo que el citado artículo 18.4 "no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la «privacidad» según el neologismo que reza en la Exposición de Motivos de la LORTAD- pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos".

Así se recoge en el Preámbulo del Proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, que por su claridad se transcribe a continuación:

"La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno.

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para

decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

A nivel legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo lugar en sus orígenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD. La Ley Orgánica 5/1992 fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta ley orgánica supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa.

Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Anteriormente, a nivel europeo, se había adoptado la Directiva 95/46/CE citada, cuyo objeto era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva".

Y en este mismo sentido se pronuncia el 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 sus 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), que tiene por objeto "proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales" (artículo 1.2.), destacando en su Considerando 1 que "la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental" y en su Considerando 10 que "para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogéneo".

Consecuentemente, el derecho a la protección de datos de carácter personal de las personas físicas es un derecho fundamental y, por tanto, situado en el máximo nivel de protección jurídica, que actualmente se encuentra regulado directamente por la normativa comunitaria, estableciendo el citado RGPD un conjunto de principios, derechos, obligaciones y una estructura organizativa tendentes a garantizar dicho derecho fundamental. Dentro de los mismos, la seguridad de la información aparece como una obligación más de los responsables y encargados del tratamiento quienes deberán aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que incluirán, entre otros factores "la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento" y "la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico" (artículo 32.2. b) y c) del RGPD).

Por lo tanto, no cabe duda de que la garantía de la seguridad de los datos personales adquiere una especial trascendencia en cuanto a su protección, pero sin que ésta se limite exclusivamente al ámbito de la seguridad de dicha información, en cuanto que la protección de datos personales tiene un ámbito mucho más extenso que abarca, como decíamos, a un conjunto de principios, derechos y obligaciones mucho más amplio.

Y todo ello bajo la garantía administrativa de las "autoridades de control", funciones que en España asume, sin perjuicio de las competencias que corresponde a las

autoridades de las Comunidades Autónomas en su ámbito competencial, la Agencia Española de Protección de Datos, que actúan con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes (Artículo 52 RGPD) y son las únicas competentes para "asesorar sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento" (artículo 57.1.c) RGPD)".

En consecuencia, esta Agencia considera conforme con la normativa de protección de datos el apartado decimocuarto.3 de la Resolución sometida a informe, en el que se prevé la adopción de medidas técnicas u organizativas apropiadas que garanticen un nivel de seguridad adecuado en función del correspondiente análisis de riesgos sin perjuicio de las previsiones recogidas en el Anexo del ENS, reguladas en el Real Decreto 311/2022, de 3 de mayo. Las medidas derivadas de dicho análisis serán las que deban implementarse en aras de la protección de datos de carácter personal (teniéndose así en cuenta lo dispuesto en el artículo 32 del RGPD relativo a la "Seguridad del Tratamiento"). Dicha regulación constituye un adecuado mecanismo de articulación entre RGPD y ENS y resulta coherente con los principios de gestión de la seguridad basada en los riesgos, vigilancia continua y reevaluación periódica recogidos en los artículos 7 y 10 del Real Decreto 311/2022, de 3 de mayo.

Resulta adecuada la incorporación expresa en el apartado decimocuarto.4 de la evaluación de impacto relativa a la protección de datos dentro de la PSI, al reconocer que la gestión de la seguridad de la información no puede desvincularse de los riesgos que los tratamientos de datos personales pueden generar para los derechos y libertades de las personas físicas. La previsión resulta coherente con los artículos 35 y 39 del RGPD, que exigen la realización de una evaluación de impacto cuando sea probable que un tratamiento entrañe un alto riesgo y atribuyen al DPD la función de asesorar sobre dicha evaluación.

De igual modo, es correcta la previsión contenida en el apartado decimocuarto.5 de la Resolución, conforme a la cual las auditorías de seguridad previstas en el Esquema Nacional de Seguridad incorporarán la revisión de las medidas técnicas y organizativas aplicables a la protección de los datos personales. Dicha previsión contribuye a garantizar una adecuada integración entre las exigencias derivadas del Real Decreto 311/2022, de 3 de mayo, y las obligaciones establecidas en los artículos 24 y 32 del Reglamento (UE) 2016/679, permitiendo verificar periódicamente la eficacia de las medidas implantadas y reforzando el principio de responsabilidad proactiva que inspira la normativa de protección de datos

En lo relativo a la figura del DPD, apartado decimotercero, debe valorarse favorablemente que la Resolución garantice la independencia funcional del DPD en el ejercicio de sus funciones, de conformidad con lo dispuesto en el artículo 38 del Reglamento (UE) 2016/679. En particular, resulta adecuada la previsión de que el Delegado no pueda recibir instrucciones respecto del desempeño de las funciones que le atribuye la normativa de

protección de datos, así como la adopción de medidas dirigidas a evitar situaciones de conflicto de intereses.

En este sentido, se considera especialmente adecuada la previsión conforme a la cual la persona designada como DPD no podrá coincidir con la persona designada Responsable de la Seguridad ni existir dependencia jerárquica entre ambas figuras, garantizándose así la necesaria separación entre las funciones de supervisión y asesoramiento en materia de protección de datos y las funciones ejecutivas relacionadas con la implantación y gestión de las medidas de seguridad de la información.

Igualmente, debe valorarse positivamente la participación del DPD, con voz, pero sin voto, en el Comité de Seguridad de la Información del INJUVE, previsto en el apartado octavo.2.b).3.º de la Resolución, así como su intervención en los procedimientos de evaluación de impacto relativos a la protección de datos cuando los tratamientos puedan entrañar un alto riesgo para los derechos y libertades de las personas físicas, contribuyendo de este modo a la efectiva aplicación de los principios de responsabilidad proactiva y protección de datos desde el diseño y por defecto previstos en los artículos 24 y 25 del Reglamento (UE) 2016/679.

Debe recordarse, no obstante, que el cumplimiento de la normativa de protección de datos corresponde al responsable del tratamiento, sin que las funciones de asesoramiento y supervisión atribuidas al DPD impliquen la asunción por éste de responsabilidades ejecutivas respecto de las decisiones adoptadas en materia de tratamiento o seguridad de los datos personales.

III

En cuanto a la gestión de la seguridad en el INJUVE, la resolución, en sus apartados sexto a decimotercero, regula adecuadamente la estructura organizativa en materia de seguridad de la información, identificando los principales órganos y figuras responsables de su implantación, supervisión y seguimiento. Entre ellos, destacan la Dirección del organismo y el Comité de Seguridad de la Información (CSI), así como la persona Responsable de la Seguridad (RSeg), las personas Responsables de la Información (RInf) y del Servicio (RSer), la persona Responsable del Sistema (RSis), las personas Administradoras de la Seguridad del Sistema y el Delegado o Delegada de Protección de Datos (DPD), quienes desempeñan funciones específicas en el marco de la Política de Seguridad de la Información para garantizar su correcta aplicación, mantenimiento y evolución, lo cual se informa asimismo favorablemente.

La Dirección del organismo constituye el máximo órgano responsable del impulso y aprobación de la Política de Seguridad de la Información y de la

dotación de los recursos necesarios para su efectiva implantación. Entre sus funciones se encuentran la aprobación de las directrices generales en materia de seguridad, el nombramiento de las personas titulares de las distintas responsabilidades previstas en la Resolución cuando así proceda, la promoción de la mejora continua del sistema de gestión de la seguridad y el impulso de las actuaciones necesarias para garantizar el cumplimiento tanto del Esquema Nacional de Seguridad como de la normativa de protección de datos personales.

Por su parte, el Comité de Seguridad de la Información (CSI) se configura como el órgano colegiado encargado de coordinar y supervisar la seguridad de la información dentro del organismo. Entre sus funciones figuran la propuesta de directrices y procedimientos de seguridad, la supervisión de la implantación de la Política de Seguridad de la Información, el seguimiento del cumplimiento del ENS, la coordinación de las actuaciones derivadas de la gestión de incidentes, auditorías y planes de mejora, así como la promoción de iniciativas de formación y concienciación. Asimismo, el Comité constituye el órgano de coordinación entre las distintas unidades implicadas en la gestión de la seguridad y puede elevar propuestas a los órganos directivos para la adopción de las medidas que resulten necesarias.

La persona Responsable de la Seguridad es la encargada de determinar, promover y supervisar la aplicación efectiva de las medidas de seguridad adoptadas por el organismo, velando por que los sistemas y servicios se adecuen a los requisitos establecidos en la Política de Seguridad y en el Esquema Nacional de Seguridad. Entre sus cometidos se encuentran el seguimiento de la implantación de las salvaguardas previstas, la propuesta de medidas correctoras y la supervisión del estado general de la seguridad. Resulta especialmente adecuada la previsión relativa a la necesaria separación de esta figura respecto de la persona Responsable del Sistema y del DPD, en aplicación del principio de diferenciación de responsabilidades y con el fin de evitar situaciones de conflicto de intereses.

Las personas Responsables de la Información y del Servicio tienen atribuidas funciones esenciales en la gestión del riesgo. Corresponde a las primeras determinar los requisitos de seguridad aplicables a la información tratada, clasificarla adecuadamente y participar en los análisis de riesgos, seleccionando y aceptando, en su caso, los riesgos residuales. A las segundas corresponde establecer los requisitos de seguridad asociados a la prestación de los servicios cuya responsabilidad ostentan, participando igualmente en los análisis de riesgos y en la aceptación de aquellos riesgos residuales que afecten a la continuidad y adecuada prestación de dichos servicios. Ambas figuras desempeñan, por tanto, un papel esencial en la implantación del modelo de gestión de la seguridad basado en el riesgo previsto en el ENS.

La persona Responsable del Sistema es quien asume la responsabilidad sobre la operación, configuración y mantenimiento técnico de los sistemas de información del organismo, garantizando la implantación efectiva de las medidas de seguridad aprobadas y supervisando el correcto funcionamiento de los sistemas bajo su responsabilidad. Esta figura no podrá coincidir con las personas Responsables de la Información, del Servicio o de la Seguridad, dando así cumplimiento al principio de diferenciación de responsabilidades previsto en el artículo 11 del Real Decreto 311/2022, de 3 de mayo.

Asimismo, la Resolución prevé la existencia de personas Administradoras de la Seguridad del Sistema, encargadas de ejecutar y gestionar las medidas técnicas y operativas necesarias para la administración segura de los sistemas de información, desarrollando sus funciones bajo la dirección de la persona Responsable del Sistema y conforme a los procedimientos y controles establecidos por la organización.

En cuanto al DPD, el apartado decimotercero regula con la necesaria amplitud su posición y funciones, en términos acordes con lo dispuesto en los artículos 37 a 39 del RGPD y en el título V de la LOPDGDD. Le corresponde informar y asesorar a los responsables del tratamiento acerca de las obligaciones que les incumben en virtud de la normativa de protección de datos, supervisar su cumplimiento, asesorar en la realización de las evaluaciones de impacto relativas a la protección de datos cuando proceda y actuar como punto de contacto con esta Agencia y con los interesados en las cuestiones relacionadas con el tratamiento de sus datos personales.

Debe valorarse favorablemente, asimismo, la previsión de que el DPD participe en el Comité de Seguridad de la Información con voz pero sin voto, garantizando de este modo su integración en la estructura organizativa de la seguridad sin menoscabo de la independencia funcional que le reconoce el artículo 38 del Reglamento (UE) 2016/679. Del mismo modo, resulta adecuada la previsión conforme a la cual dicha figura no podrá coincidir con la persona Responsable de la Seguridad ni mantener una relación de dependencia jerárquica que pudiera comprometer el ejercicio independiente de sus funciones.

Finalmente, debe reiterarse que la designación del DPD deberá efectuarse atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y de la práctica en materia de protección de datos, así como a su capacidad para desempeñar las funciones que tiene encomendadas, de conformidad con lo dispuesto en el artículo 37 del RGPD y en el artículo 34 de la LOPDGDD.

IV

Por lo demás, según se advierte, el texto que se informa evidencia la evolución de las políticas de seguridad de la información desde modelos basados en la mera verificación formal del cumplimiento hacia un enfoque sustentado en el análisis de riesgos, la evaluación del impacto sobre los derechos y libertades de las personas físicas y el principio de responsabilidad proactiva previsto en el artículo 5.2 del Reglamento (UE) 2016/679. Dicho enfoque queda plasmado en las previsiones relativas al análisis de riesgos, a la determinación de las medidas de seguridad apropiadas y a la realización de evaluaciones de impacto relativas a la protección de datos, resultando coherente con lo dispuesto en los artículos 24, 32 y 35 del citado Reglamento, así como con la consideración de los riesgos a que se refiere su considerando 75.

La determinación de las funciones atribuidas a las distintas figuras responsables de la seguridad de la información y al Delegado o Delegada de Protección de Datos respeta el necesario conocimiento que este último debe poseer acerca de la Política de Seguridad de la Información, participando en su implantación desde las funciones de asesoramiento y supervisión que le atribuye expresamente el Reglamento (UE) 2016/679. En este sentido, debe valorarse favorablemente la previsión de su participación en el Comité de Seguridad de la Información con voz y sin voto, lo que permite su adecuada integración en la estructura organizativa sin menoscabo de la independencia funcional que le reconoce el artículo 38 del citado Reglamento.

Asimismo, debe valorarse positivamente que la Resolución deslinde adecuadamente los ámbitos de actuación del DPD y de la persona Responsable de la Seguridad, evitando la coincidencia de ambas funciones y descartando relaciones de dependencia jerárquica que pudieran comprometer la autonomía e independencia exigibles al primero.

Por otra parte, la Resolución atribuye al Responsable del tratamiento las obligaciones derivadas de la aplicación de los principios de responsabilidad proactiva, protección de datos desde el diseño y por defecto, seguridad del tratamiento y realización, en su caso, de las evaluaciones de impacto relativas a la protección de datos. Corresponde, por tanto, al Responsable del tratamiento la adopción de las decisiones necesarias para garantizar el cumplimiento de la normativa de protección de datos, sin perjuicio de que las medidas técnicas y organizativas se desarrollen por las distintas figuras integradas en la estructura de seguridad del organismo.

En este contexto, la función del DPD consiste en prestar al Responsable del tratamiento el asesoramiento y la asistencia necesarios en el proceso de adopción de dichas medidas y supervisar el cumplimiento de las obligaciones establecidas por la normativa de protección de datos personales, actuando asimismo como punto de contacto con los interesados y con la Agencia Española de Protección de Datos.

Debe señalarse, no obstante, que, a diferencia de otros textos análogos informados por esta Agencia, la Resolución no incorpora una previsión específica relativa a la identificación expresa de la persona, organismo o unidad que ostente la condición de Responsable o Encargado del tratamiento en los términos de los apartados 7 y 8 del artículo 4 del Reglamento (UE) 2016/679, si bien atribuye al Responsable del tratamiento las obligaciones materiales derivadas de la aplicación de dicha normativa.

Finalmente, aun cuando la Resolución integra adecuadamente la gestión de riesgos y la realización de evaluaciones de impacto en el marco general de la Política de Seguridad de la Información, no contiene una referencia expresa a la necesidad de atender a las directrices, orientaciones o herramientas elaboradas por la Agencia Española de Protección de Datos en el desarrollo de tales actuaciones, previsión que sí aparece recogida en otros textos análogos examinados por este Servicio Jurídico.

V

En conclusión, la Resolución analizada cumple con las exigencias en materia de protección de datos personales, al prever expresamente el pleno sometimiento a la normativa aplicable en esta materia, garantizar el respeto al conjunto de principios relativos al tratamiento previstos en el artículo 5 del Reglamento (UE) 2016/679 e incorporar los principios de responsabilidad proactiva y de protección de datos desde el diseño y por defecto. Asimismo, contempla la realización del correspondiente análisis de riesgos y, en su caso, de las evaluaciones de impacto relativas a la protección de datos en aquellos tratamientos que puedan entrañar un alto riesgo para los derechos y libertades de las personas físicas, de conformidad con el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre.

Todas estas previsiones se contienen fundamentalmente en el apartado decimocuarto de la Resolución, dedicado específicamente a la protección de los datos personales, sin perjuicio de las funciones atribuidas a las personas Responsables de la Información y del Servicio en materia de análisis y gestión de riesgos.

Asimismo, la Resolución articula adecuadamente la relación entre el Esquema Nacional de Seguridad y la normativa de protección de datos personales, estableciendo que, cuando del correspondiente análisis de riesgos resulte necesario, las medidas derivadas de la aplicación del Reglamento (UE) 2016/679 prevalecerán sobre las previstas con carácter general en el Esquema Nacional de Seguridad, garantizando así el adecuado cumplimiento de las exigencias derivadas del artículo 32 del citado Reglamento. Esta prevalencia

debe entenderse en el sentido de que las exigencias derivadas del correspondiente análisis de riesgos pueden determinar la necesidad de complementar o reforzar las medidas previstas en el Esquema Nacional de Seguridad cuando estas resulten insuficientes para afrontar los riesgos identificados, poniendo así de manifiesto el carácter integrado y complementario de ambos marcos normativos.

Por otra parte, debe valorarse favorablemente que el texto evidencie una evolución desde modelos de cumplimiento basados en la mera verificación formal de requisitos hacia un enfoque sustentado en el análisis de riesgos, la evaluación del impacto sobre los derechos y libertades de las personas físicas y el principio de responsabilidad proactiva previsto en el artículo 5.2 del Reglamento (UE) 2016/679, enfoque que resulta plenamente coherente con lo dispuesto en los artículos 24, 32 y 35 del citado Reglamento, así como con la consideración de los riesgos a que se refiere su considerando 75.

Por último, la Resolución contempla con la debida atención que el Delegado o Delegada de Protección de Datos desempeñe labores de asesoramiento y supervisión en el ámbito de aplicación de la Política de Seguridad de la Información, prestando apoyo a los responsables del tratamiento en la identificación de riesgos, la adopción de medidas de protección, el asesoramiento en materia de evaluaciones de impacto relativas a la protección de datos y la verificación de la correcta implantación y ejecución de las medidas adoptadas. Asimismo, su participación en el Comité de Seguridad de la Información con voz y sin voto resulta acorde con las funciones que le atribuye la normativa de protección de datos y compatible con la independencia funcional que le reconoce el artículo 38 del Reglamento (UE) 2016/679. Del mismo modo, la separación funcional prevista entre dicha figura y la persona Responsable de la Seguridad contribuye a preservar la autonomía e independencia exigibles al DPD en el ejercicio de sus funciones.

Todo lo anterior se encuentra debidamente contemplado en la Resolución que se informa.

No obstante, se considera conveniente sugerir una mejora técnica en la redacción del apartado decimocuarto.2, a fin de adecuar plenamente su terminología a la empleada por el Reglamento (UE) 2016/679. En concreto, se propone sustituir la referencia a la adopción de «medidas técnicas u organizativas apropiadas» por la expresión «medidas técnicas y organizativas apropiadas», en línea con lo dispuesto en los artículos 24, 25 y 32 del citado Reglamento. De este modo, quedaría expresamente reflejado que la protección de los datos personales exige la adopción conjunta y complementaria de medidas de ambas naturalezas, reforzando así la coherencia terminológica del texto con la normativa europea de protección de datos.

Finalmente, en lo relativo a la figura del Delegado o Delegada de Protección de Datos, las previsiones contenidas en el apartado decimotercero de la Resolución resultan conformes con la normativa de protección de datos, si bien ha de reiterarse que su designación debe efectuarse de conformidad con lo dispuesto en el artículo 37 del Reglamento (UE) 2016/679 y en el artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre, atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y de la práctica en materia de protección de datos, así como a su capacidad para desempeñar las funciones que tiene encomendadas.

Por todo lo expuesto, esta Agencia considera que el proyecto de Resolución por la que se aprueba la Política de Seguridad de la Información en el ámbito de la Administración Digital del organismo autónomo Instituto de la Juventud resulta, con carácter general, conforme con las previsiones establecidas en el Reglamento (UE) 2016/679, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, y en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

En consecuencia, se informa favorablemente la Resolución sometida a consulta, sin perjuicio de las observaciones efectuadas en el presente informe.