IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

ARTÍCULO

Las normas ISO/IEC como mecanismos de responsabilidad proactiva en el Reglamento General de Protección de Datos*

Jorge Viguri Cordero
Universitat Jaume I

Fecha de presentación: noviembre de 2020
Fecha de aceptación: abril de 2021
Fecha de publicación: octubre de 2021

Resumen

El mercado de la certificación ha experimentado un auge sin precedentes tras la entrada en vigor y ulterior aplicación del RGPD. Ello obliga a poner de relieve la relevancia de estos mecanismos como elementos claves en la prevención de potenciales violaciones de la seguridad de los datos personales. En el presente trabajo examinamos cómo la naturaleza técnica de estos instrumentos ha cedido hacia su corregulación a los efectos de garantizar una adaptación eficiente a los continuos cambios de una gran tipología de productos, servicios o sistemas. Pretende proporcionarse una panorámica holística sobre la práctica totalidad de estándares que afectan a las dimensiones de privacidad y protección de datos, concretándose en aquellos que dimanan del estándar internacional de la serie ISO/IEC 27000, específicamente, la ISO/IEC 27001 (Seguridad de la Información) y 27701 (Gestión de la Información de Privacidad). Estándares que suponen un primer punto de partida relevante encuadrado dentro de la responsabilidad proactiva, dotando a las organizaciones de mecanismos eficaces para demostrar el cumplimiento de las disposiciones del RGPD.

Palabras clave

mecanismos de certificación, responsabilidad proactiva, RGPD, ISO/IEC 27001, ISO/IEC 27701

Tema

Derecho constitucional / europeo

* Este artículo ha sido elaborado en el marco de los proyectos de investigación del Ministerio de Ciencia e Innovación (RTI2018-095367-B-I00) y de la Conselleria d'Innovació, Universitats, Ciencia i Innovació Digital de la Generalitat Valenciana (AICO/2019/205). Por su parte, ha sido revisado y actualizado durante la estancia de investigación en la Universitat Rovira i Virgili (01/03-30/07/2021), financiada por la Conselleria de Innovación, Universidades, Ciencia y Sociedad Digital de la Generalitat Valenciana (BEST/2021/049).

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

ISO/IEC standards as mechanisms of proactive responsibility in the General Data Protection Regulation

Abstract

The certification market has experienced an unprecedented rise after the entry into force and the effective application of the GDPR. This forces us to closely highlight the relevance of these mechanisms as key prevention elements of personal data breaches. In this paper, we examine how the technical nature of these instruments has given way to co-regulation for efficient adaptation to continuing changes with regard to a wide range of products, services or systems. To this end, we aim at providing a holistic overview of almost every standards that affect the privacy and data protection dimensions, specifically those that derive from the international reference standard ISO/IEC 27000 (series), specifically, ISO/IEC 27001 (Information Security) and 27701 (Privacy Information Management). Standards that represent a first relevant starting point framed within the proactive responsibility, providing organisations with some effective instruments to demonstrate GDPR compliance.

Keywords

certification mechanisms, proactive responsibility, GDPR, ISO/IEC 27001, ISO/IEC 27701

Topic

Constitutional/European Law

1. Planteamiento de la cuestión

El constante desarrollo de los productos, servicios y sistemas de Tecnologías de la Información (TI) ha motivado, en los últimos tiempos, la creación y actualización de mecanismos de certificación existentes, los cuales conceden a los operadores jurídicos la capacidad de adelantarse y prevenir potenciales violaciones en la seguridad de los datos personales. Se trata de iniciativas que, tras la efectiva aplicación del Reglamento General de Protección de Datos (RGPD) el 25 de mayo de 2018, se coronan como una de las herramientas esenciales para adaptar un amplio catálogo de productos, servicios y sistemas TI a los continuos cambios que acontecen y garantizar, consecuentemente, su máxima coherencia con la legislación de protección de datos.

Su implementación responde a la perentoria necesidad de que autoridades supervisoras u organismos de certificación –acreditados en sede nacional– contemplen mecanismos capaces de certificar a los controladores y procesadores sobre el cumplimiento de la normativa de protección de datos, concediendo una distinción en forma de sellos o marcados registrados y comúnmente protegidos que gozan de un considerable grado de notoriedad por las partes interesadas. Un cometido que pretende dar cumplimiento al art. 24.1.º RGPD, que exige al responsable del tratamiento la aplicación de «medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento».

Ahora bien, la adhesión a un mecanismo de certificación no supone el fiel cumplimiento de las disposiciones legales, sino que goza de una presunción de cumplimiento en lo que atañe a «las obligaciones por parte del responsable del tratamiento» (art. 42.3.º RGPD). Estos instrumentos proporcionan una mayor seguridad a las partes interesadas a los efectos de demostrar el cumplimiento de la normativa de protección de datos y, consiguientemente, reducir o incluso evitar el régimen sancionador ante el incumplimiento de esta normativa. Tan es así, que estos se encuentran inexorablemente vinculados no solo al principio de responsabilidad proactiva o *accountability* del art. 5.2 RGPD[1], sino también a la garantía de la seguridad del tratamiento, la cual insta a que el responsable y el encargado del tratamiento implementen criterios relativos a la seguridad de tratamiento, es decir, «medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo» (art. 32.1º RGPD).

Por ende, aunque la certificación se encuadra como mecanismo fundamentalmente voluntario (art. 42.3º RGPD), esta contempla medidas preventivas muy relevantes para asegurar el respeto de la legislación de protección de datos, asegurando entre otras cuestiones, la seguridad y la portabilidad de los datos. De hecho, como reconoce el art. 83.2º j) RGPD, la adhesión a mecanismos de certificación «se tendrá debidamente en cuenta» a la hora de fijar la cuantía de la multa.

El problema radica en que el mercado actual de la certificación presenta una serie de déficits estructurales que ha lastrado su desarrollo eficaz en los últimos años. Precisamente, la Comisión Europea (CE) se mostraba muy crítica con el excesivo despliegue de certificaciones en el mercado, aludiendo al escaso conocimiento de las partes interesadas en relación a la identificación de aquellas normas técnicas más relevantes.[2] Un supuesto abordado por la doctrina europeísta, que ha identificado, como principales déficits, la generalizada indisponibilidad de información sobre los criterios técnicos de los estándares, la ausencia de supervisión reglamentaria o la falta de control efectivo en el uso indebido por parte de terceros no autorizados.[3]

En este punto, esta manifiesta falta de seguridad jurídica no ha impedido que, en los últimos tiempos, hayan irrumpido en el mercado un conjunto de esquemas y estándares de referencia certificables por parte de organizaciones que operan con los datos de los ciudadanos de la Unión Europea (UE). Un auge que ha venido acompasado gracias a la contundente acción del CEPD que, en 2019, determinó que una operación susceptible de tratamiento debía reunir *datos personales*, los *sistemas técnicos*, esto es, la infraes-

1. Rallo Lombarte (2019), pág. 49; Martínez Martínez, (2019), pág. 317.
2. Comisión Europea, Data Protection Certification Mechanisms, Study on Articles 42 and 43 of the Regulation (EU) 2016/679. Final report, febrero de 2019, págs. 16 y sigs [en línea] https://ec.europa.eu/info/sites/info/files/data_protection_certification_mechanisms_study_final.pdf [Fecha de consulta: 23 de abril de 2021].
3. Rodrigues (2018); Rodrigues, Barnard-Wills, Wright, De Hert y Papakonstantinou (2013); Rodrigues, Wright y Wadhwa (2013).

tructura empleada en el procesamiento de tales datos, así como los *procesos* vinculados con las operaciones de procesamiento.[4]

Paralelamente, su éxito también se ha radicado en las medidas de apoyo e impulso directo por parte de las Autoridades de Protección de Datos europeas (APD), que comenzaron a publicar esquemas de certificación en el plano nacional. Ese mismo año, la AEPD aprobó un pionero Esquema de certificación de Delegados de Protección de Datos (Esquema AEPD-DPD)[5], un marco potestativo de certificación que reúne las exigencias y el rigor adecuados para determinar quien dispone del conocimiento y habilidades suficientes para actuar como DPD de acuerdo con los estándares que exige el RGPD.

Es más, esta iniciativa ha sido concretada en Cataluña, donde la Escuela de Administración Pública de Cataluña (EAPC), conjuntamente con la Autoridad de Protección de Datos catalana (APDCAT), diseñaron el «Curso para Delegado de Protección de Datos de la Administración y de su sector público»[6]. Se trata de la primera certificación promovida en ámbito autonómico para certificar la cualificación profesional de los DPD de la administración y del sector público catalán y que se une a la contundente acción de otras APD europeas –como la alemana (Datenschutzaudit beim ULD)[7] o francesa (CNIL)[8]– que ya habían desarrollado esquemas de certificación en este sentido.

Si bien, al margen del modelo de certificación de personas, la finalidad de este artículo radica en analizar las certificaciones relativas a procesos y, concretamente, las conocidas normas dimanantes de la Organización Internacional de Normalización (ISO)/Comisión Electrotécnica Internacional (IEC). Estas han ido correlativamente adaptando sus criterios a los requisitos legales del RGPD con la clara intención de dar respuesta a una alta demanda del mercado relativa al cumplimiento de requisitos técnicos y legales relacionados con la seguridad de la información (SI). Se trata de estándares de referencia a nivel mundial que incluyen las mejores prácticas reconocidas por esta Organización internacional para garantizar el cumplimiento del RGPD, por lo que corresponde a los controladores y procesadores de datos determinar si la oferta de estándares ISO/IEC resulta pertinente y necesaria para demostrar que la organización en cuestión, cumple efectivamente con los criterios legales relativos a privacidad y protección de datos.

2. La certificación como mecanismo de naturaleza técnica y su progresiva aproximación hacia el ámbito legal

Uno de los principales retos a los que se enfrenta la certificación es su enorme amplitud por cuanto no se trata *stricto sensu* de un concepto únicamente técnico ni tampoco jurídico. Esto nos lleva a examinar cuál ha sido y es la naturaleza de estos mecanismos con objeto de comprender mejor el potencial alcance que estos ofrecen. Una de las primeras cuestiones que conviene examinar estriba en la propia definición de la norma susceptible de ser certificada. El Reglamento Europeo sobre la Normalización Europea 1025/2012 fue pionero en definir el concepto de certificación desde un enfoque técnico en el apartado 1º del art. 2º en los siguientes términos: «la especificación técnica adoptada por un organismo de normalización reconocido, de aplicación repetida o continua, cuya observancia no es obligatoria, y que reviste diversas formas: a) "norma internacional": norma adoptada por un organismo internacional de normalización; b) "norma europea": norma adoptada por una organización europea de normalización; c) "norma armonizada": norma europea adoptada a raíz de una petición de la Comisión para

4. Comité Europeo de Protección de datos. Directrices 1/2018 sobre certificación e identificación de criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento 2016/679, 4 de junio de 2019 (versión 3.0), pág. 13 [en línea] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_es.pdf [Fecha de consulta: 23 de abril de 2021].
5. Agencia Española de Protección de Datos. Esquema de certificación de delegados de protección de datos de la Agencia Española de Protección de Datos (esquema AEPD-DPD) [en línea] https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf [Fecha de consulta: 23 de abril de 2021].
6. Generalitat de Cataluña. La Escuela de Administración Pública y la Autoridad Catalana de Protección de Datos presentan el primer curso de certificación de Delegados de Protección de Datos del sector público catalán, 29 de enero de 2020.
7. https://www.datenschutzzentrum.de/audit/
8. https://www.cnil.fr/fr/certification-des-competences-du-dpo-la-cnil-adopte-deux-referentiels.

la aplicación de la legislación de armonización de la Unión y d) "norma nacional": norma adoptada por un organismo nacional de normalización».

Por lo tanto, este concepto –tradicionalmente adscrito a una vertiente técnica– ha lastrado su pleno encaje como una norma jurídica vinculante a todos los efectos. No obstante, fue la Directiva 2016/1148 sobre ciberseguridad la que modificó su denominación, definiendo este concepto en el art. 19 como aquellas «normas y especificaciones aceptadas a nivel europeo o internacionalmente que sean pertinentes en materia de seguridad de las redes y sistemas de información».

Por consiguiente, la preeminencia de los estándares técnicos comenzó a ceder desde un concepto puramente técnico hacia otro más próximo a la regulación normativa[9], lo cual ha tenido efectos significativos tanto en su propia denominación como en sus ulteriores efectos jurídicos. Tan es así que, en el presente, tales mecanismos pueden asociarse a verdaderas normas técnico-jurídicas[10].

En efecto, esta tipología de certificación comenzó a impulsarse para dotar de una mayor transparencia al funcionamiento interno de las organizaciones, habida cuenta de que muchas de ellas operaban con una gran tipología de datos personales y los usuarios generalmente desconocían el uso posterior que se hacía de los mismos. Fue articulada como un procedimiento para garantizar el cumplimiento de los requisitos específicos en materia de SI –como en el caso de los estándares que integran la serie ISO/IEC 27000 a la que haremos referencia más adelante– y aumentar considerablemente la confianza de los usuarios en el comercio electrónico[11].

Tras la entrada en vigor del RGPD en 2016, la certificación marcó un *antes y un después*, erigiéndose como una de las medidas alternativas más eficaces para fortalecer la protección de los datos personales de las personas físicas, facilitar la libre circulación de los datos personales y reducir las persistentes obstaculizaciones relacionada con la ineficiencia en el conjunto de administraciones públicas. Buena prueba de ello, el Considerando 100 RGPD previó expresamente la apuesta por la implementación de medidas de certificación con objeto de solventar las serias trabas de cierta entidad a las que se había enfrentado la certificación, facilitando a las partes interesadas la evaluación específica del nivel de protección de datos de las operaciones de procesamiento.

Sin embargo, el proceso de implementación de estándares coherentes con el RGPD no fue una realidad hasta su efectiva aplicación el 25 de mayo de 2018, momento a partir del cual se produce una publicación concatenada de normas e iniciativas de certificación que buscan promover la protección de privacidad desde el inicio y la prevención de brechas de la seguridad de los datos personales. En este preciso momento, se produjo una transición desde el enfoque tradicional de autorregulación hacia otro corregulatorio. Un modelo en el que la adhesión a un mecanismo de certificación aprobado puede emplearse como elemento que demuestre el cumplimiento de las obligaciones del presente Reglamento (Considerando 81). De esta forma, el citado Reglamento se focaliza en reconocer a la certificación como herramienta proactiva para demostrar su cumplimiento, delegando a los operadores técnicos y jurídicos su ulterior desarrollo e implementación práctica.

No cabe obviar que la certificación reviste carácter de cláusula abierta o de especificación en el RGPD de tal forma que, con independencia de los estándares reconocidos internacionalmente, este ha dotado del margen de maniobra nacional necesario a los Estados miembros para determinar su extensión y alcance concreto. En este contexto, las respectivas APD europeas han empleado todo su conocimiento a fin de crear y evaluar aquellos criterios de certificación más pertinentes para garantizar el cumplimiento de la normativa de protección de datos.

Por lo que se refiere a España, la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), de 5 de diciembre de 2018 en su art. 39 únicamente detalla las condiciones de acreditación de instituciones de certificación, sin especificar cuestiones esenciales para garantizar el

9. En octubre de 2020, se planteó mediante consulta pública la revisión holística de la citada Directiva, incluyendo la actualización de este concepto ligado a la normativa ISO/IEC y sus homónimos nacionales.
10. Sobre la divergencia conceptual de los estándares y su vinculación, remitimos al estudio de tesis doctoral: Pascual Huerta (2017), págs. 42 y 43.
11. En el año 2012, la Comisión reconoció la necesidad de incrementar la confianza de los consumidores en las compras transfronterizas en línea mediante la adopción de medidas políticas apropiadas. Comisión Europea, COM(2012) 225 final, Bruselas, 2 de mayo de 2012.

correcto funcionamiento de estos mecanismos, como son: el periodo máximo de duración, el tipo de publicidad accesible, la revocación, la sujeción a futuros actos delegados o actos de ejecución de la Comisión o la figura de los organismos de certificación previstos en el art. 43 RGPD[12].

Consecuentemente, la LOPDGDD requiere, en todo momento, una lectura síncrona con el RGPD para promover la comprensión práctica de estos mecanismos y, por ende, garantizar la seguridad jurídica en lo que atañe al ordenamiento jurídico nacional. Aún con todo, no es menos cierto que el mercado global de la certificación ha ido más allá, actualizando y creando estándares internacionales que se adaptan al nuevo contexto vinculante del RGPD. Entre sus criterios de certificación, contemplan referencias expresas al RGPD aunque carecen del nivel de especificación requerido por las legislaciones nacionales de protección de datos, evidenciando un punto de partida relevante para cumplir con aspectos esenciales previstos por la norma europea como es, entre otras cuestiones, la SI.

3. Los estándares técnicos vinculados al cumplimiento eficaz del Reglamento General de Protección de Datos

3.1. La certificación sobre protección de la información, privacidad o datos personales: un mercado muy extendido a la par que difuso

El RGPD apuesta decididamente por la implementación de mecanismos de certificación de certificación en su art. 42, principalmente, de aquellos específicos en el marco de la privacidad y de la protección de los datos personales que, como hemos hecho referencia anteriormente, son creados o respaldados por las respectivas APD en sede nacional. Ello, sin perjuicio de que puedan encontrarse multitud de estándares internacionales ISO/IEC que, efectivamente, prevén referencias concretas a las dimensiones de privacidad y protección de datos.

En primer lugar, el estándar certificable ISO/IEC 27001 contempla aquellos requisitos técnicos y operativos necesarios para reducir el riesgo de vulneración de las disposiciones del RGPD[13]. Esta certificación también permite orientar, dirigir y concretar de qué manera se llevan a las Evaluaciones de Impacto en la Protección de Datos Personales (EIPD) en el seno de una organización. De hecho, el informe de EIPD puede incluir documentación sobre las medidas adoptadas para el tratamiento de riesgos, por ejemplo, en relación con acciones dimanantes del empleo de un Sistema de Gestión de la Seguridad de la Información (SGSI) si la organización está certificada conforme a la norma ISO/IEC 27001 o de un Sistema de Gestión de Información sobre Privacidad (PIMS), conforme al estándar ISO/IEC 27701[14].

Sobre el particular, merece igualmente traer a colación el estándar ISO/IEC 29134, que proporciona pautas relevantes sobre cómo realizar una EIPD[15] y cómo estructurar su correspondiente informe. Una certificación reciente para aquellas organizaciones interesadas en garantizar que sus actuaciones y procedimientos resultan eficientes en cuanto al efectivo cumplimiento de las evaluaciones de impacto. Se trata de una norma de referencia para las organizaciones que quieren cumplir con el RGPD; es más, entre todas las organizaciones que están certificadas para tal fin, un 68% cumplen con este estándar (Informe ISO, 2018)[16].

12. Para un primer análisis sobre los mecanismos de certificación y su impacto en España, véase: Viguri Cordero (2019), pág. 391; Rabazo Auñón (2019), págs. 549-568.
13. UNE-EN e ISO/IEC 27001: 2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. A lo largo de los sucesivos pies de págs., aquellas normas que carecen de tipicidad UNE-EN supone que la norma todavía no ha sido normalizada en España por la Asociación Española de Normalización y Certificación (AENOR).
14. ISO/IEC 27701: 2019. Técnicas de seguridad. Extensión a ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información de privacidad. Requisitos y directrices. Para un análisis de este estándar y su aplicación en el ámbito de la empresa, véase: Burillo Zamora (2020).
15. Estas son vinculantes cuando el procesamiento de datos puede suponer un alto riesgo para los derechos y libertades de las personas físicas (art. 35.4 RGPD). UNE-EN e ISO/IEC 29134: 2020. Tecnología de la información. Técnicas de seguridad. Directrices para la evaluación del impacto de la privacidad (ISO/IEC 29134: 2017)
16. https://www.iso.org/files/live/sites/isoorg/files/about%20ISO/annual_reports/en/annual_report_2018_en.pdf. [Fecha de consulta: 23 de abril de 2021].

Además de estos, confluyen otros estándares que responden a demandas más concretas como el ISO/IEC 29151, por el que establece objetivos y pautas para implementar controles que cumplan con los requisitos identificados por una evaluación de riesgo e impacto relacionada con la protección de la información de identificación personal (PII)[17]. Por su parte, los estándares ISO 9001 relativa al Sistema de Gestión de la Calidad (SGC)[18] e ISO 22301 sobre el Sistema de Gestión de la Continuidad de Negocio (SGCN)[19] contemplan otros aspectos trasversales relevantes a estos efectos como la satisfacción de los consumidores y usuarios, incluyendo la eficacia de la gestión de las reclamaciones en general y los incidentes que afectan a los datos personales en particular.

Igualmente, las organizaciones deben concretar una política de riesgo en el ámbito de la SI, la cual puede encauzarse mediante la certificación de la IEC 31010[20], que complementa a la tradicional ISO 31000[21] y que permite que estos desarrollen, implementen y mejoren un marco de referencia de forma continua para integrar el proceso para la gestión del riesgo en los procesos globales de dirección, estrategia y planificación[22].

Este último estándar, junto al IEC 31010, proveen de orientación sobre la selección y adopción de técnicas útiles para la evaluación y gestión del riesgo en distintos contextos de la organización donde existe un supuesto crítico de inseguridad. Es más, la norma ISO/IEC 27017 sobre Controles de Seguridad para Servicios en la nube[23] se perfecciona con la recientemente ratificada ISO/IEC 27018[24], que certifica aquellos requisitos para la protección de la información de identificación personal en estos sistemas.

No obstante, la ISO/IEC 27001 sobre SGSI ha incorporado directamente en su "Anexo D" nuevas cláusulas de certificación que se aproximan al concepto de "responsabilidad proactiva", uno de los ejes vertebradores del RGPD. En esta misma línea, la ISO/IEC 27701 supone una extensión de la anterior para la gestión de la privacidad o PIMS y prevé un conjunto de cláusulas coherentes con aquellos aspectos más destacables del RGPD, incluyendo:

- los principios relativos al tratamiento (art. 5 RGPD);
- la obligación de la transparencia de la información, comunicación y las modalidades de ejercicio de los derechos del interesado (art. 12 RGPD);
- el ejercicio de los derechos de Acceso, Rectificación, Supresión, Oposición, Portabilidad y Limitación (arts. 13 y ss. RGPD);
- la notificación de una violación de la seguridad de los datos personales a la autoridad de control (art. 33 RGPD);
- la EIPD (art. 35 RGPD);
- la designación del DPD (art. 37 RGPD) o;
- la concreción de las condiciones para efectuar las transferencias internacionales de datos en sintonía con las atribuciones del RGPD en materia de certificación (arts. 42.1 y 46 RGPD).

Aparte de estos estándares, merece especial énfasis otros relevantes para la implementación de sistemas de gestión de la protección de datos, como el BS 10012 relativo al "Sistema de Gestión de Información Personal". Un están-

17. ISO/IEC 29151: 2017. Tecnología de la información - Técnicas de seguridad - Código de prácticas para la protección de la información de identificación personal.
18. UNE-EN e ISO 9001: 2015. Sistemas de gestión de la calidad. Requisitos.
19. UNE-EN e ISO 22301: 2015. Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Especificaciones.
20. IEC 31010: 2019. Gestión de Riesgos: Técnicas de Evaluación de Riesgos.
21. UNE e ISO 31000: 2018. Gestión del riesgo. Directrices.
22. La certificación de las normas ISO 31000 e IEC 31010 resulta sumamente eficiente para aquellas organizaciones que deben efectuar una Evaluación de Impacto de Protección de Datos (EIPD) conforme a lo dispuesto en el art. 35 del RGPD, tomando en consideración que la gestión de riesgos se enmarca dentro de la actividad ordinaria de las organizaciones.
23. ISO/IEC 27017: 2015. Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube. Actualmente en proyecto de norma en España por parte de AENOR.
24. UNE-EN e ISO/IEC 27018: 2020 (Ratificada). Tecnología de la Información. Técnicas de seguridad. Código de práctica para la protección de identificación personal (PII) en nubes públicas que actúan como procesadores PII (ISO/IEC 27018:2019).

dar británico alineado con los principios del RGPD que proporciona un marco de mejores prácticas para implementar un PIMS mediante la descripción de los requisitos básicos que las organizaciones deben tener en cuenta al recopilar, almacenar, procesar, conservar o eliminar los registros personales de los interesados. Como reconoce BSI Group, este estándar se integra fácilmente con los restantes estándares análogos y permite ayudar a identificar y gestionar los riesgos de la información personal, a la par que cumplir eficazmente con la legislación de protección de datos, incrementar sustancialmente la confianza de los clientes y elevar la reputación de la organización certificada[25].

3.2. La norma ISO/IEC 27001 y su extensión en la norma ISO/IEC 27701

La relación entre el estándar ISO/IEC 27001 sobre el SGSI resulta plenamente coherente con la actividad de certificación (art. 42 RGPD) por cuanto se centra en la necesidad de adopción de medidas organizativas y técnicas necesarias para garantizar un nivel elevado en la SI tanto de personas, procesos y tecnología.

En este sentido, las medidas de seguridad previstas en la ISO 27001 deben implementarse a la luz de los principios de *integridad* y *disponibilidad* (art. 5.f) RGPD) y en clara yuxtaposición con el concepto de resiliencia, entendiéndose como la capacidad reactiva de la organización ante incidentes susceptibles de comprometer la SI[26]. Ahora bien, a diferencia de las acciones susceptibles de aplicación por parte del responsable de tratamiento (art. 24 RGPD), este estándar certifica de forma independiente la gestión de la PII que lleva a cabo una organización, por lo que puede emplearse como mecanismo que demuestre el cumplimiento eficaz las disposiciones de la normativa de protección de datos. De este modo, insta a las organizaciones que pretenden certificarse a que designen una persona que asuma la responsabilidad del SGSI para los fines previstos en el Considerando 85 y art. 5.2º RGPD, es decir, que sean estas las que impulsen las respectivas medidas necesarias y pertinentes para proteger los datos personales tras las oportunas evaluaciones periódicas que identifican amenazas y vulnerabilidades concretas que pueden afectar a los activos de su información. Una acción que ha sido especificada por las autoridades de supervisión en el plano nacional,[27] tomando como referencia la identificación inequívoca del responsable (art. 30 RGPD) y el nivel de seguridad adecuado (art. 32.2 RGPD).

Finalmente, también debe prestarse atención a la *Política de Protección de Datos* prevista en esta norma. Un requisito que, pese a encontrarse dentro del ámbito de la SI, insta a que las organizaciones la contemplen en el marco de sus procedimientos de procesamiento y tratamiento de datos a fin de proveer medidas estratégicas sobre el cumplimiento del RGPD. Ciertamente, aunque esta norma refuerza sustancialmente la SI y protege los datos personales en el seno de la organización, no incluye referencias expresas al RGPD, principalmente, las relativas a los derechos de los interesados que reconocen los arts. 12 y ss. Ciertamente, se trata de especificaciones de técnicas que pretenden minimizar los incidentes asociados a los riesgos de seguridad.

En aras de identificar una norma técnica que contemple criterios jurídicos dimanantes del RGPD, debemos retrotraernos a agosto de 2019, cuando fue publicada la ISO/IEC 27701 sobre la Gestión de la Información de Privacidad. Este reciente estándar extiende la norma de referencia ISO/IEC 27001 hacia la aplicación y perfeccionamiento de un Sistema de Gestión de Información de Privacidad (PIMS)», el cual ha sido catalogado por el SEPD como aquellos «que ayudan a dar a las personas más control sobre sus datos personales. Los PIMS permiten a las personas administrar sus datos personales en sistemas de almacenamiento seguros,

25. https://www.bsigroup.com/en-GB/BS-10012-Personal-information-management/ [Fecha de consulta: 6 de mayo de 2021]. 26 Sáiz Peña (2019), pág. 389.
26. Sáiz Peña (2019), pág. 389.
27. En el caso de España, la AEPD describe los procedimientos para proceder a la realización de un análisis de riesgos con objeto de establecer medidas de seguridad y control para garantizar los derechos y libertades de las personas. Véase AEPD: Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD [en línea] https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf [Fecha de consulta: 23 de abril de 2021].

locales o en línea, y compartirlos cuando y con quien elijan»[28].

Por consiguiente, no solo orienta a los responsables y encargados de tratamiento sobre la definición de un marco de gestión para una implementación de la obligaciones del RGPD –desde un enfoque basado en la eficiencia y eficacia–, sino que especifica los aspectos sobre privacidad que deben adoptar las organizaciones. Constituye una norma de carácter subsidiario a la norma ISO/IEC 27001, por lo que es necesario que la organización cuente previamente con esta certificación a los efectos de extender los requisitos técnicos de SI a aquellos otros adscritos a la dimensión de privacidad/protección de datos. Conexión que supone un avance trascendental en la certificación, pues permite constatar un elevado grado de coherencia con los fines de los arts. 42 y 43 RGPD. Ello, aunque Lachaud advierta de las lagunas de las normas certificables en relación con el cumplimiento efectivo del mencionado Reglamento, motivo por el que las autoridades de supervisión deben colmar las brechas existentes entre los dos marcos y aclarar sus relaciones en un futuro a corto plazo[29].

Precisamente, en aras de garantizar el cumplimiento del PIMS, la organización debe asegurarse con anterioridad a su certificación de que los datos personales administrados por la entidad reúnan los requisitos del SGSI establecidos en la norma ISO/IEC 27001. Un requisito que se diferencia claramente de la seguridad de los datos del art. 32 RGPD por cuanto este no exige su cumplimiento previo. Dicho esto, cabe apuntar que el mencionado estándar técnico concreta la SI con un distinto enfoque al previsto legalmente en el Reglamento, previniendo y abordando la probabilidad y gravedad de los riesgos de los derechos y libertades de las personas físicas desde una doble vertiente:

a) Por un lado, contempla referencias expresas al RGPD con objeto de exigir a las organizaciones certificadas bajo este estándar el cumplimiento de los requisitos de protección de datos de manera específica a su contexto, procesamiento y nivel de riesgo. Estas abarcan desde el diseño de aquellas medidas de seguridad aplicables a los datos personales (art. 32.1 RGPD), la gestión de las consecuencias de una violación de la seguridad de los datos personales (art. 34.1 RGPD), la pertinencia en llevar a cabo una EIPD (art. 35.2 RGPD) o la contratación de un DPD (art. 37.2 RGPD). En estos dos últimos casos, en aquellos supuestos no vinculantes que prevé el apartado 1.º de los arts. 35 y 37 RGPD.

b) Por otro lado, el citado estándar define sus propios requisitos que, con cierta frecuencia, difieren de sus homólogos en el RGPD. Por ejemplo, los requisitos previstos en la subcláusula 7.2.6 aplicables a los encargados del tratamiento de los datos son facultativos en el estándar ISO/IEC, mientras que en Reglamento son plenamente vinculantes (art. 28 RGPD). Además, las normas ISO no aseguran el pleno cumplimiento de las salvaguardas de protección de datos, razón por la que la subcláusula 6.1.3 b) de la norma ISO/IEC 27001 contempla excepciones a la aplicación de controles de privacidad si con ello se aseguran las relaciones con los encargados de tratamiento –a condición de que esté justificada en la declaración de aplicabilidad requerida por la metodología basada en el riesgo–.

Es más, otras normas como la ISO/IEC 29100 sobre Protección de Datos de Información Personal[30] tampoco contempla ningún retraso para notificar una violación de la seguridad de los datos a las autoridades de supervisión en la subcláusula 6.13.3. Esto dista directamente del art. 33.1 RGPD, que requiere efectuar tal notificación «a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas», así como comunicarlo directamente a los interesados potencialmente afectados: «Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida» (art. 34.1 RGPD).[31]

28. Supervisor Europeo de Protección de Datos. Opinión 9/2016 sobre Sistemas de Gestión de Información Personal. Hacia un mayor empoderamiento del usuario en la gestión y el procesamiento de datos personales, 20 de octubre de 2016 [en línea] https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf [Fecha de consulta: 23 de abril de 2021].
29. Lachaud (2020), pág. 4.
30. ISO/IEC 29100:2011 (Revisada en 2017). Tecnología de la información. Técnicas de seguridad. Marco de privacidad.

Ahora bien, el responsable de los datos puede llevar a cabo una EIPD cada vez que considere que este procedimiento es útil o necesario para evaluar el riesgo del procesamiento de datos. Al efecto, la norma ISO/IEC 27701 prevé en la subcláusula 7.2.6 que las organizaciones certificadas respeten las legislaciones aplicables. Si bien, lo hace de forma muy amplia, sin especificar cómo afecta a cada organización candidata, que deberán cumplir con las disposiciones del RGPD y las respectivas legislaciones nacionales allí donde operen.

4. Reflexiones conclusivas

El mercado de la certificación actual ha sufrido una transformación sustancial en los últimos años, desde las meras iniciativas de autorregulación hacia su emplazamiento como marco técnico con directas implicaciones en el ámbito jurídico, concretamente, en el derecho a la protección de datos personales. Con ello, los estándares susceptibles de ser certificados por parte de una organización cumplen la función esencial de prevenir potenciales violación de la seguridad de los datos personales y aproximar sus procesos internos al cumplimiento efectivo del RGPD.

Entre todos los estándares presentes en el mercado de la certificación, las organizaciones que apuesten por esta vía de protección de los derechos deberían focalizar sus esfuerzos en la certificación de la norma ISO/IEC 27001, la cual protege eficazmente la SI, reduce cualquier amenaza cibernética y guarda un alto nivel de coherencia con el RGPD. Es más, tras esta primera certificación, las organizaciones cuentan con la posibilidad de certificarse conforme al reciente estándar ISO/IEC 27701, un (sub) estándar que concreta la primera norma –de carácter más general– hacia una exhaustiva labor de integración de las disposiciones más relevantes del RGPD.

Con todo, debe destacarse que el ámbito de aplicación de esta ISO/IEC 27001 resulta más concreto que el RGPD, por cuanto se centra en aquellas obligaciones que deben cumplir las organizaciones para garantizar la SI. En esta línea, su concreción en la ISO/IEC 27701 pretende promover la gestión eficaz de los riesgos de SI de las organizaciones que ya están certificadas conforme a la ISO/IEC 27001 a fin de implementar las mejores prácticas internacionales en relación con procesos que incluyen una amplia tipología de información que excede de los datos personales a los efectos del citado Reglamento.

Finalmente, no debe obviarse que pese a que se trata de una iniciativa privada que adapta una gran amalgama de productos, servicios o sistemas al cumplimiento efectivo del RGPD, sus elevados costes pueden comprometer la viabilidad de esos estándares, especialmente, para aquellas organizaciones o empresas de menor tamaño o con recursos más limitados. Es por ello por lo que, al margen de las normas ISO/IEC analizadas, deberán ser las APD nacionales las que impulsen –todavía más– nuevos esquemas de certificación conjuntas a medio plazo que fomenten y garanticen el máximo respeto de la legislación de protección de datos.

31 Dentro de la familia ISO/IEC 29100, se encuentra la ISO/IEC 29184:2020 sobre declaraciones de confidencialidad en línea y el consentimiento. Un consentimiento que, como demuestra Harshvardhan y Krog (2021), difiere ampliamente del consentimiento libremente prestado e inequívoco que regula el art. 4 RGPD.

Referencias bibliográficas

BURILLO ZAMORA L. (2020). «Efecto y modo de implantación de la nueva ISO/IEC 27701:2019 en el ámbito empresarial», *La Ley privacidad,* núm. 3 (Enero-marzo 2020).

CHATZIPOULIDIS, A.; TSIAKIS, T.; KARGIDIS, T. (2029). «A readiness assessment tool for GDPR compliance certification». *Computer Fraud & Security*, núm. 8 [en línea] DOI: https://doi.org/10.1016/S1361-3723(19)30086-7 [Fecha de consulta: 23 de abril de 2021].

LACHAUD, E. (2020). ISO/IEC 27701: Threats and Opportunities for GDPR Certification [en línea] https://ssrn.com/abstract=3521250 [Fecha de consulta: 23 de abril de 2021].

MARTÍNEZ MARTÍNEZ, R. (2019). «El principio de responsabilidad proactiva y la protección de datos desde el diseño y por defecto». En: GARCÍA MAHAMUT, R.; TOMÁS MALLÉN, B. (eds.). *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales*. Valencia: Tirant Lo Blanch.

PANDIT HARSHVARDHAN J., KROG G. P. (2021). «Comparison of notice requirements for consent between ISO/IEC 29184:2020 and GDPR». *Journal of Data Protection & Privacy*, vol. 4, núm. 2, pp. 193-204 [en línea] http://doi.org/10.5281/zenodo.4444926 [Fecha de consulta: 7 de mayo de 2021].

PASCUAL HUERTA, P. (2017). *La génesis del derecho fundamental a la protección de datos Personales* [tesis doctoral]. Madrid: Universidad Complutense [en línea] https://eprints.ucm.es/id/eprint/43050/1/T38862.pdf [Fecha de consulta: 23 de abril de 2021].

RABAZO AUÑÓN, N. (2019). «Los códigos de conducta y las certificaciones en el RGPD (Arts. 40-43 RGPD. Arts. 38-39 y Disposición transitoria segunda LOPDGDD». En: LÓPEZ CALVO, J. (coord.). *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Madrid: Wolters Kluwer.

RALLO LOMBARTE, A. (2019). «El nuevo derecho de protección de datos». *Revista Española de Derecho Constitucional*, núm. 116 [en línea] https://doi.org/10.18042/cepc/redc.116.02 [Fecha de consulta: 23 de abril de 2021].

RODRIGUES, R. (2018). «Conclusion: What Next for Privacy Seals?». En: RODRIGUES, R.; PAPAKONSTANTINOU, V. (eds.). *Privacy and Data Protection Seals. Information Technology and Law Series,* vol. 28. T.M.C. Asser Press, The Hague [en línea] https://doi.org/10.1007/978-94-6265-228-6_9 [Fecha de consulta: 23 de abril de 2021].

RODRIGUES, R.; BARNARD-WILLS, D.; WRIGHT, D.; DE HERT, P.; PAPAKONSTANTINOU, V. (2013). *EU Privacy seals project, Inventory and Analysis of Privacy Certification Schemes: Final Report Study* Deliverable 1.4, Comisión Europea. Luxemburgo: Oficina de publicaciones de la Unión Europea [en línea] https://publications.jrc.ec.europa.eu/repository/handle/JRC85092 [Fecha de consulta: 23 de abril de 2021].

RODRIGUES, R.; WRIGHT, D.; WADHWA, K. (2013). «Developing a privacy seal scheme (that works)». *International Data Privacy Law*, vol., 3, núm. 2 [en línea] https://doi.org/10.1093/idpl/ips037 [Fecha de consulta: 23 de abril de 2021].

SÁIZ PEÑA, C. A. (2019). «Seguridad de los datos, evaluación de impacto, códigos de conducta y certificación». En: RALLO LOMBARTE, A. (ed.). *Tratado de Protección de Datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.* Valencia: Tirant lo Blanch.

VIGURI CORDERO, J. (2019). «Los mecanismos de certificación en la Ley orgánica de Protección de Datos y garantía de los derechos digitales: un nuevo paradigma a la luz del RGPD». En: GARCÍA MAHAMUT, R.; TOMÁS MALLÉN, B. (eds.). *El Reglamento General de Protección de Datos. Un enfoque*

nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales. Valencia: Tirant Lo Blanch.

VIGURI CORDERO, J. (2015). «Los mecanismos de certificación (códigos de conducta, sellos y marcas)». En: RALLO LOMBARTE, A.; GARCÍA MAHAMUT, R. (eds.). *Hacia un nuevo derecho europeo de protección de datos*. Valencia: Tirant lo Blanch.

Cita recomendada

VIGURI CORDERO, Jorge (2021). «Las normas ISO/IEC como mecanismos de responsabilidad proactiva en el Reglamento General de Protección de Datos». *IDP. Revista de Internet, Derecho y Política*, núm. 33 (octubre). UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i33.376366

Sobre el autor

Jorge Viguri Cordero
Profesor ayudante doctor de la Universitat Jaume I (UJI).
Departamento de Derecho Público. Derecho Constitucional
Miembro del grupo de investigación PRODADEF (Protección de Datos y Derechos Fundamentales)
JC2331DD - (964 728715)
jviguri@uji.es

Jorge Viguri Cordero es profesor ayudante doctor (acreditado a contrato doctor) en el área de Derecho Constitucional por la Universitat Jaume I. Ha sido investigador en los proyectos europeos CRISP (Evaluation and Certification schemes for Security Products) y Phaedra II (Improving Practical and Helpful Cooperation between Data Protection Authorities), ambos financiados por la Comisión Europea.
Entre sus líneas de investigación activas destacan el derecho a la protección de datos de carácter personal y el derecho a la protección internacional. Autor de la monografía "Seguridad y protección de datos en el Sistema Europeo Común de Asilo" (Tirant lo Blanch, 2020) y de mas de una decena de artículos en diversas revistas científicas de impacto, así como capítulos de libros.